Extended Communication Server

Manuel d'Installation et de Configuration

Version 4.1

Juillet 2008

Alcatel-Lucent Office Communication Solutions
All Rights Reserved © Alcatel-Lucent 2008

Informations légales :

Alcatel, Lucent, Alcatel-Lucent et le logo Alcatel-Lucent sont des marques d'Alcatel-Lucent. Toutes les autres marques appartiennent à leurs propriétaires respectifs.

Les informations présentées sont sujettes à modification sans préavis.

Alcatel-Lucent ne peut être tenu pour responsable de l'inexactitude de ces informations.

Copyright © 2008 Alcatel-Lucent. Tous droits réservés.

Le marquage CE indique que ce produit est conforme aux directives communautaires suivantes :
- 89/336/CEE (Compatibilité électromagnétique)
- 73/23/CEE (Sécurité Basse Tension)
- 1999/5/CE (R&TTE)

CE

Sommaire

Manuel d'Installation et de Configuration

Chapitre 1
Procédure d'installation

1.1 Objectif de ce document 1.1
1.2 Présentation du produit 1.1
1.3 Présentation matérielle 1.2
1.4 Profils utilisateurs et interfaces graphiques 1.3
1.4.1 Interface graphique d'administration 1.4
1.4.2 Bureau Virtuel 1.6
1.5 Présentation de l'installation et de la configuration 1.7
1.6 Prérequis à l'installation 1.8

Chapitre 2
Installation et démarrage

2.1 Introduction 2.1
2.2 Démarrage via l'accès direct 2.1
2.3 Démarrage à partir d'un PC local 2.2
2.4 Accès limité à l'interface d'administration 2.4

Chapitre 3
Déverrouillage du pack logiciel

3.1 Principes 3.1
3.2 Déverrouillage du pack logiciel 3.1

Chapitre 4
Configuration du réseau

4.1 Principes 4.1
4.2 Paramètres Réseau Généraux 4.2
4.3 Connexions réseau 4.3
4.3.1 Généralités sur la configuration des connexions réseau 4.3
4.3.2 Connexion WAN ADSL PPPoE 4.4
4.3.3 Connexion LAN Ethernet 4.5
4.3.4 Connexion de pont Ethernet 4.7
4.3.5 Connexion LAN Ethernet DMZ 4.8
4.3.6 Connexion Alias LAN Ethernet 4.8
4.4 Service DHCP 4.9
4.4.1 Configuration globale 4.10
4.4.2 Machines déclarées 4.11
4.4.3 Baux DHCP 4.11
4.5 Proxy distant 4.11

Chapitre 5
Enregistrement, activation et mises à jour

5.1 Généralités 5.1
5.2 Enregistrement et génération de la clé d'activation 5.1
5.3 Activation de la licence 5.2
5.4 Mises à jour logicielles 5.3

Chapitre 6
Gestion des utilisateurs

6.1 Généralités 6.1
6.2 Gestion des groupes d'utilisateurs et des comptes utilisateurs 6.2
6.2.1 Création de groupes d'utilisateurs 6.2
6.2.2 Création de comptes utilisateurs 6.3
6.3 Droits des utilisateurs 6.3

Chapitre 7
Gestion de la sécurité

7.1 Présentation 7.1
7.2 Gestion du firewall 7.1
7.2.1 Généralités 7.1
7.2.2 Paramètres avancés 7.3
7.3 Gestion du serveur proxy 7.6
7.3.1 Services proxy 7.6
7.3.2 Activation du service proxy cache 7.6
7.3.3 Contrôle d'accès au Web 7.7
7.3.4 Filtrage Web 7.7
7.3.5 Configuration du client 7.9
7.3.6 Statistiques du proxy cache 7.10
7.4 Gestion des certificats 7.10

7.4.1 Présentation 7.10
7.4.2 Création d'un certificat utilisateur 7.11
7.4.3 Utilisation d'un certificat 7.12
7.4.4 Activation de la regénération automatique des certificats 7.13

Chapitre 8
Convergence voix/données

8.1 Généralités 8.1
8.2 Activation de la convergence voix/données 8.2
8.3 Récupération des informations 8.3

Chapitre 9
Gestion de la messagerie

9.1 Généralités 9.1
9.2 Messagerie interne 9.1
9.3 Extension du service à Internet 9.1
9.4 Configuration pour un client lourd de messagerie 9.3
9.5 Paramètres supplémentaires 9.3
9.5.1 Noms de domaine 9.3
9.5.2 Anti-relais / Autorisation de relais 9.5
9.5.3 Messagerie distante 9.6
9.5.4 Filtrage des mails 9.6

Chapitre 10
Hébergement Web

10.1 Présentation de l'hébergement de sites 10.1
10.2 Configuration du service d'hébergement 10.2
10.2.1 Indication du webmaster 10.2
10.2.2 Création du site 10.4
10.2.3 Association d'une base de données au site 10.5
10.2.4 Résolution de noms 10.5
10.3 Chargement du site sur le serveur 10.7
10.3.1 Chargement via FTP 10.7
10.3.2 Chargement via le voisinage réseau Microsoft 10.7
10.4 Limites et restrictions 10.7

Chapitre 11
Mobilité

11.1 Push Mobile 11.1
11.1.1 Présentation 11.1
11.1.2 Pré-requis 11.1
11.1.3 Activation du service Push Mobile 11.1
11.1.4 Configuration du service Push Mobile 11.3
11.1.5 Configuration des accès utilisateur au service Push Mobile 11.3
11.2 Téléphonie SIP sur Internet 11.3
11.2.1 Introduction 11.3
11.2.2 Configuration de base pour la téléphonie SIP sur Internet 11.5
11.2.3 Configuration d'interopérabilité avec OmniPCX Office 11.7
11.2.4 Ajout d'un bouton Click to call sur le site Web 11.8

Chapitre 12
Sauvegarde et restauration

12.1 Généralités 12.1

12.2 Procédure de sauvegarde 12.1
12.2.1 Définition d'un profil de sauvegarde 12.1
12.2.2 Exécution d'une sauvegarde 12.3
12.3 Procédure de restauration 12.4

Chapitre 13
Annexes

13.1 Comment établir un devis 13.1
13.2 Comment commander 13.1

Chapitre

1

Procédure d'installation

1.1 Objectif de ce document

L'Extended Communication Server propose une interface Web conviviale à l'attention des administrateurs. Cette interface graphique s'accompagne d'une aide en ligne détaillée contenant suffisamment d'informations pour réaliser les tâches d'administration les plus courantes.

Le présent document vise à guider l'administrateur lors des premières étapes d'installation et de configuration, afin qu'il puisse installer le serveur sur le réseau du client et autoriser la communication entre les utilisateurs finaux. Une fois ces opérations effectuées, l'administrateur pourra découvrir par lui-même les multiples fonctions et paramètres de l'Extended Communication Server et se référer à l'aide en ligne chaque fois qu'il aura besoin d'informations supplémentaires.

1.2 Présentation du produit

Conçu pour les petites et moyennes entreprises (PME), l'Extended Communication Server est une solution de collaboration et de mobilité puissante qui offre :

- un ensemble d'outils de collaboration permettant un partage efficace des informations dans le cadre d'un projet ou au sein d'une équipe, d'un groupe ou de l'entreprise toute entière ;
- un accès mobile et sécurisé à l'ensemble des outils de collaboration de l'entreprise, en toute simplicité ;
- une solution de communication unifiée intégrée à l'OmniPCX Office ;
- une gestion sécurisée du Web et un déploiement aisé ;
- un ensemble complet de serveurs informatiques ;
- un serveur d'hébergement Web.

L'Extended Communication Server est un composant phare des solutions de communication Office.

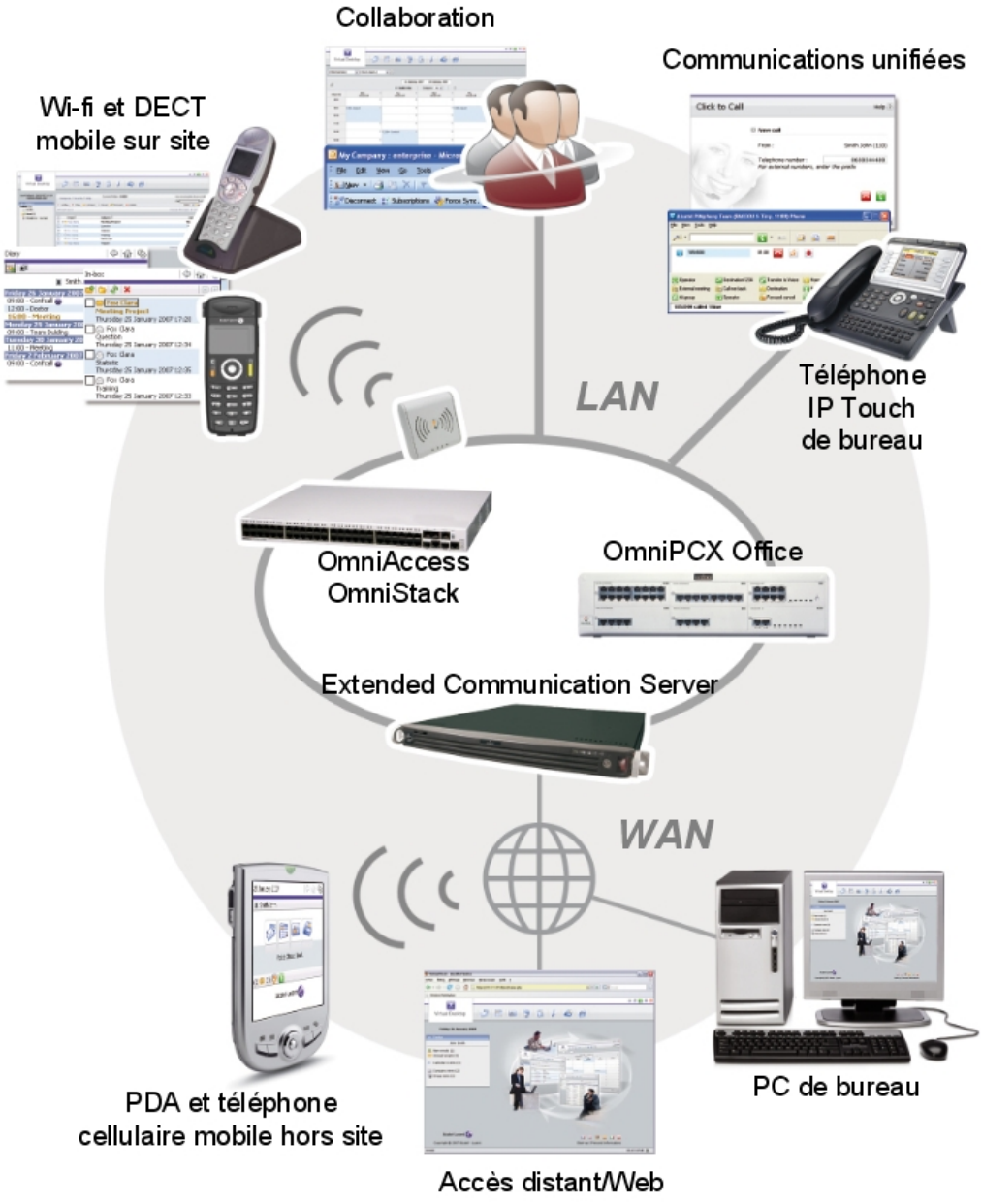


Figure 1.1 : Position au sein des solutions de communication Office

1.3 Présentation matérielle

La plate-forme matérielle de l'Extended Communication Server est disponible dans deux versions :

- L'**édition Compact** est un serveur de bureau, également montable en rack, conçu pour les petites entreprises de 25 utilisateurs maximum.

- L'**édition Premium** est une plate-forme montée sur rack qui s'adresse aux moyennes entreprises comprenant entre 25 et 200 utilisateurs.

Les deux versions de l'Extended Communication Server sont gérées de manière identique. Sauf mention contraire expresse, toutes les informations et procédures mentionnées dans le présent document s'appliquent à ces deux versions.

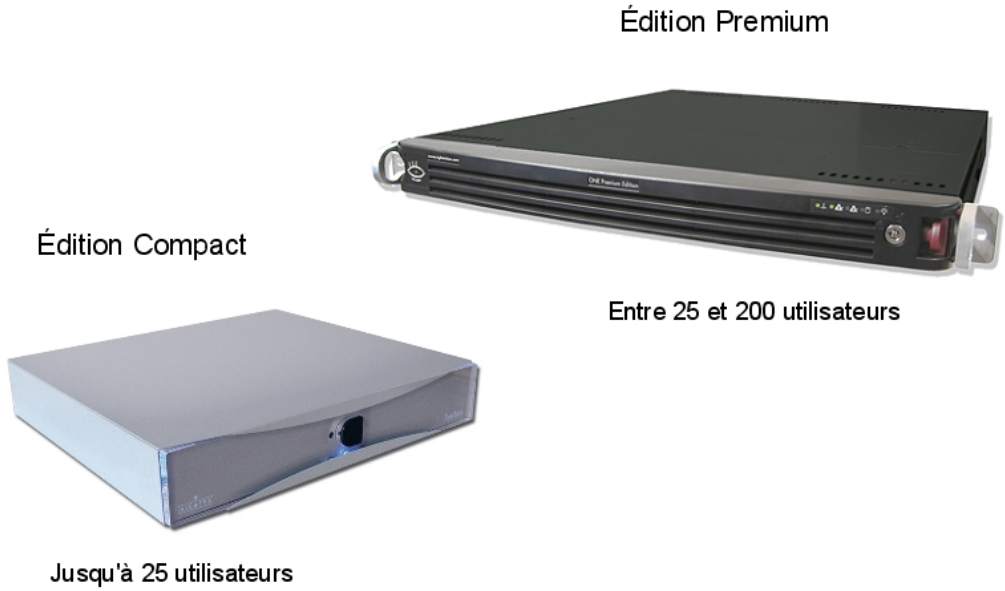


Figure 1.2 : Plates-formes matérielles

Le tableau suivant présente les caractéristiques des plates-formes des éditions Compact et Premium.

tableau 1.1 : Caractéristiques des plates-formes matérielles

Édition Compact	**Édition Premium**
- Processeur Via C3 1,5 GHz - RAM 512 Mo - Disque dur 160 Go 7 200 tr/min - 3 interfaces Ethernet RJ-45 10/100 Mbits/s - 1 port PCI (*) - 1 port de console - 1 port VGA - 1 port d'imprimante	- Processeur Intel® Core 2 Duo E6320 - Jeu de puces Intel E3000 (Mukilteo-2) - SDRAM DDR2-667 2 Go - 3 disques durs SATA-2 250/500 Go échangeables à chaud - 3 interfaces réseau Gigabit (RJ-45) - Carte graphique ATI ES 1000 - DVD-ROM extra-plat - 2 ports USB 2.0 en façade - 1 port COM série - Alim. 300 Watts

1.4 Profils utilisateurs et interfaces graphiques

L'Extended Communication Server est accessible par trois types d'utilisateurs :

- Un administrateur qui, depuis l'interface graphique d'administration, gère les comptes utilisateurs et contrôle toutes les ressources et fonctions du système, notamment l'architecture du réseau, les mesures de sécurité, les dispositifs de messagerie électronique et l'accès à Internet.
- Des utilisateurs, qui gèrent leur propre compte et accèdent aux services disponibles via une interface graphique appelée Bureau Virtuel. Ces services sont également accessibles depuis le Bureau Virtuel Mobile, à partir de postes nomades comme des PDA (Personal Digital Assistant).
- Des administrateurs délégués (utilisateurs disposant de droits d'administration limités), qui ont accès à la fois au Bureau Virtuel et à un nombre réduit de menus de l'interface graphique d'administration.

Le navigateur Web constitue le point d'accès à l'interface graphique d'administration et au Bureau Virtuel. Lorsque l'utilisateur se connecte, l'Extended Communication Server propose l'une ou l'autre de ces interfaces, en fonction du nom d'utilisateur et du mot de passe saisis. L'administrateur délégué peut basculer d'un affichage à l'autre au moyen de boutons graphiques auxquels il est le seul à pouvoir accéder.

Note :
L'administrateur n'est pas enregistré dans la base de données des utilisateurs et n'est donc pas réellement considéré comme un utilisateur. Pour pouvoir accéder au Bureau Virtuel, il doit se créer un compte utilisateur.

1.4.1 Interface graphique d'administration

L'interface graphique d'administration est accessible via un navigateur Web standard (Internet Explorer, Mozilla Firefox, Netscape Navigator, etc.) et nécessite une connexion sécurisée (https). L'administrateur peut se connecter depuis le réseau local ou à distance, via Internet. Il peut aussi accéder à l'interface d'administration depuis un écran branché directement sur le serveur, et utiliser un clavier et une souris.

Simple d'utilisation, l'interface d'administration propose quatre menus principaux pour la gestion de l'Extended Communication Server, des services, des utilisateurs finaux, ainsi que pour le contrôle et la surveillance du trafic.

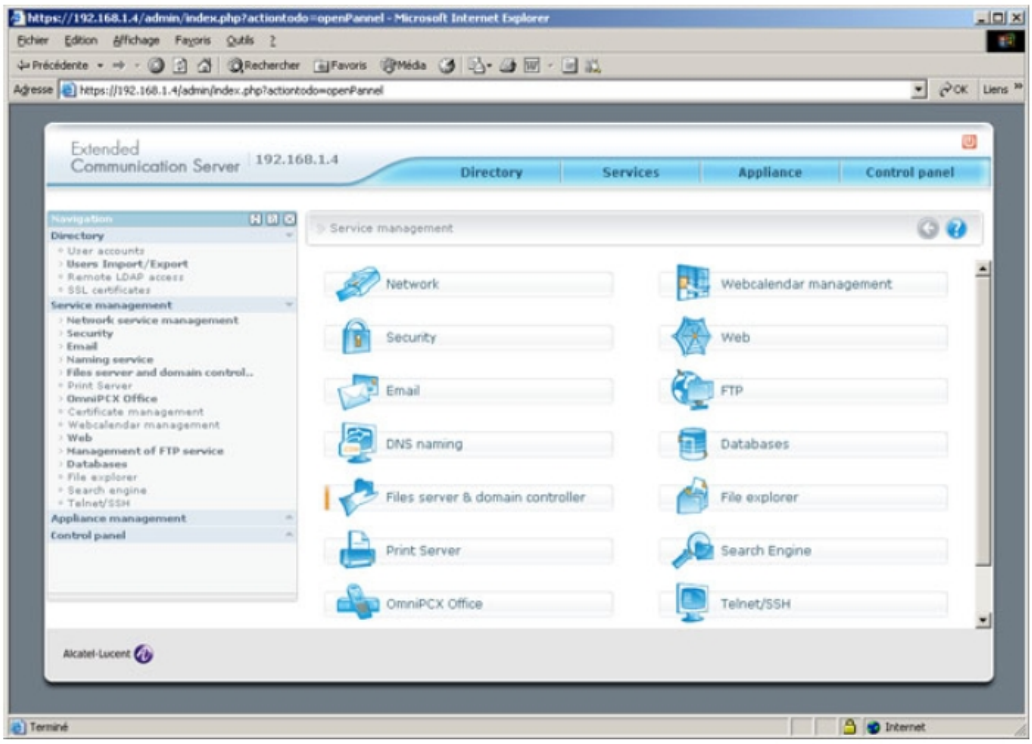


Figure 1.3 : Interface graphique d'administration

Chaque menu intègre des sous-menus, accessibles depuis le panneau gauche ou via un clic sur les icônes associées. L'administrateur a la possibilité de réduire ce panneau pour faire uniquement apparaître les icônes.

Un bouton d'aide ( ) est disponible à tout moment, quel que soit le menu ou le sous-menu affiché, et permet d'ouvrir une fenêtre pop-up contenant des informations contextuelles utiles. Chaque page d'aide peut être imprimée.

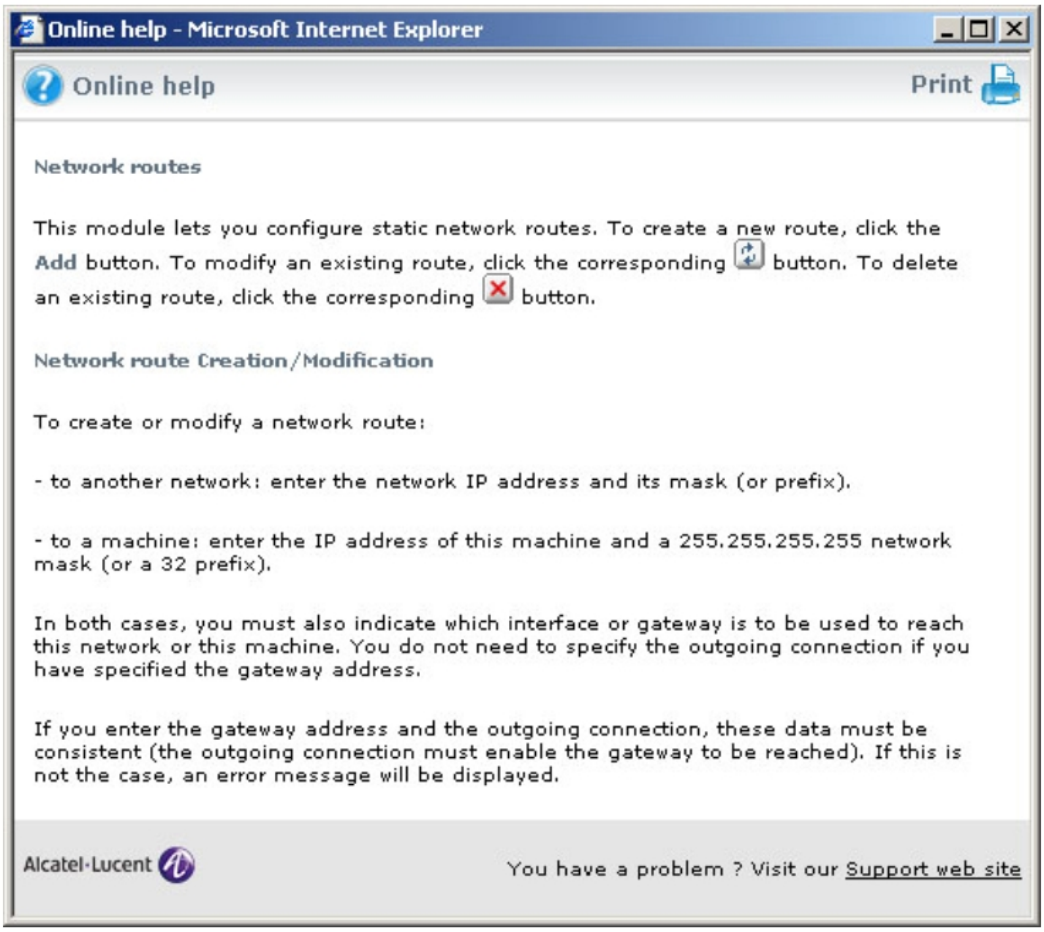

Online help - Microsoft Internet Explorer
Online help
Print
Network routes
This module lets you configure static network routes. To create a new route, click the Add button. To modify an existing route, click the corresponding button. To delete an existing route, click the corresponding button.
Network route Creation/Modification
To create or modify a network route:
- to another network: enter the network IP address and its mask (or prefix).
- to a machine: enter the IP address of this machine and a 255.255.255.255 network mask (or a 32 prefix).
In both cases, you must also indicate which interface or gateway is to be used to reach this network or this machine. You do not need to specify the outgoing connection if you have specified the gateway address.
If you enter the gateway address and the outgoing connection, these data must be consistent (the outgoing connection must enable the gateway to be reached). If this is not the case, an error message will be displayed.
Alcatel·Lucent
You have a problem ? Visit our Support web site

Figure 1.4 : Exemple d'aide en ligne contextuelle

L'interface intuitive et l'aide en ligne représentent autant de moyens pour l'administrateur de découvrir les multiples fonctions et paramètres de l'Extended Communication Server.

1.4.2 Bureau Virtuel

Les procédures de connexion au Bureau Virtuel et à l'interface d'administration sont identiques, à la différence que dans le premier cas, le nom et le mot de passe employés sont ceux d'un utilisateur standard.

Une fois connecté au Bureau Virtuel, l'utilisateur peut gérer ses propres services, comme ses messageries Web, son agenda, ses contacts, ses sites favoris, etc.

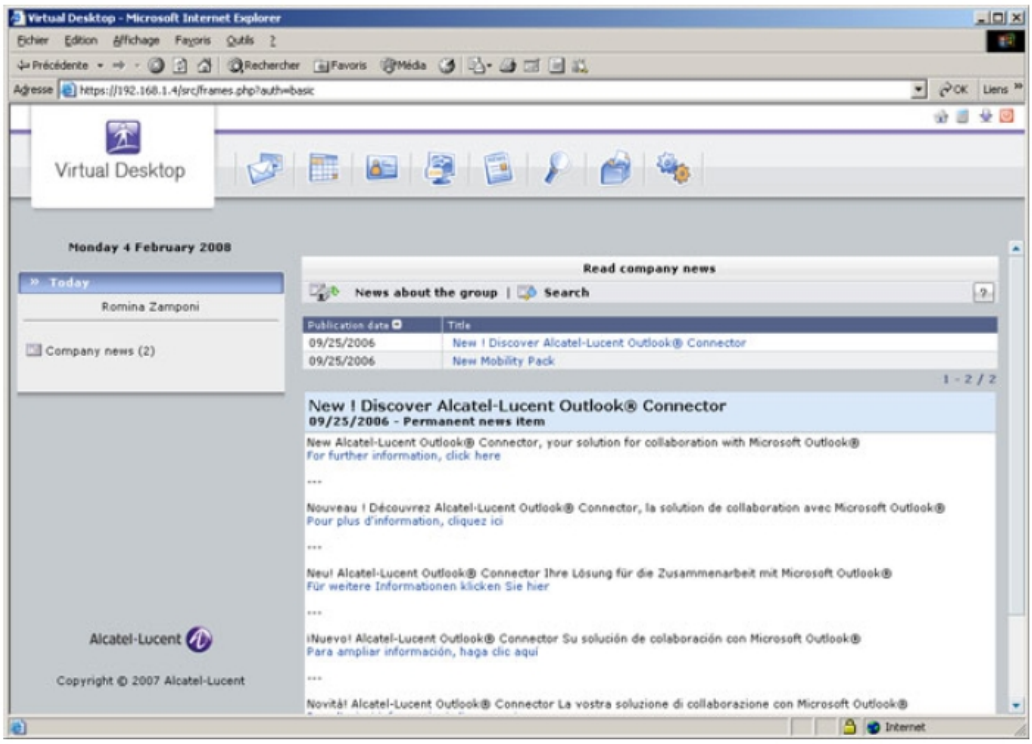

Virtual Desktop - Microsoft Internet Explorer
Virtual Desktop
Monday 4 February 2008
Today
Romina Zamponi
Company news (2)
Read company news
News about the group | Search
Publication data
Title
09/25/2006
New ! Discover Alcatel-Lucent Outlook® Connector
09/25/2006
New Mobility Pack
New ! Discover Alcatel-Lucent Outlook® Connector
09/25/2006 - Permanent news item
New Alcatel-Lucent Outlook® Connector, your solution for collaboration with Microsoft Outlook®
For further information, click here
Nouveau ! Découvrez Alcatel-Lucent Outlook® Connector, la solution de collaboration avec Microsoft Outlook®
Pour plus d'information, cliquez ici
Neu! Alcatel-Lucent Outlook® Connector Ihre Lösung für die Zusammenarbeit mit Microsoft Outlook®
Für weitere Informationen klicken Sie hier
¡Nuevo! Alcatel-Lucent Outlook® Connector Su solución de colaboración con Microsoft Outlook®
Para ampliar información, haga clic aquí
Novità! Alcatel-Lucent Outlook® Connector La vostra soluzione di collaborazione con Microsoft Outlook®
Alcatel-Lucent
Copyright © 2007 Alcatel-Lucent

Figure 1.5 : Aperçu du Bureau Virtuel

Le Bureau Virtuel propose un ensemble de commandes d'interface intuitives facilitant la gestion des services, ainsi qu'une aide en ligne détaillée fournissant des informations lorsque nécessaire.

1.5 Présentation de l'installation et de la configuration

Ce section présente les premières étapes qu'un administrateur doit suivre lors de l'installation de l'Extended Communication Server chez le client et de la configuration du réseau et des services.

Ces étapes sont décrites plus en détail dans les chapitres suivants.

tableau 1.2 : Chronologie succincte de l'installation et de la configuration

Ordre recommandé	**Étapes**	**Objectifs**
Étape 1	Installation et démarrage	Démarrer le serveur et accéder à l'interface graphique d'administration
Étape 2	Déverrouillage du pack logiciel	Déverrouiller le pack logiciel et accéder aux menus de l'interface d'administration
Étape 3	Configuration du réseau	Installer le serveur sur le réseau du client et accéder au Web

Ordre recommandé	Étapes	Objectifs
Étape 4	Enregistrement, activation du logiciel et mises à jour	Accéder au support technique, activer la licence complète et profiter des derniers packs logiciels
Étape 5	Gestion des utilisateurs	Créer les comptes et gérer les droits des utilisateurs
Étape 6	Gestion de la sécurité	Contrôler les flux entrants et sortants
Étape 8	Convergence voix/données	Associer les comptes utilisateurs aux dispositifs de téléphonie
Étape 9	Gestion de la messagerie	Permettre aux utilisateurs d'envoyer et de recevoir des messages sur le LAN et via Internet

D'autres fonctions utiles peuvent être installées ultérieurement (voir chapitres à la fin du présent document).

1.6 Prérequis à l'installation

Nous vous recommandons tout d'abord de prendre connaissance de ce document et d'étudier précisément les besoins du client.

Les points suivants devront ensuite être pris en considération au moment de la préparation de l'installation de l'Extended Communication Server :

- Architecture du réseau :
  - LAN
  - DMZ (Demilitarized Zone)
  - Accès Internet
- Plan d'adressage IP, notamment :
  - Machines locales nécessitant une adresse statique
  - Planification dynamique de l'affectation
- Informations fournies par le FAI (Fournisseur d'accès Internet), comme les adresses IP des serveurs DNS
- Nom de domaine public
- Gestion des utilisateurs, notamment :
  - Groupes d'utilisateurs
  - Comptes utilisateurs
  - Droits d'accès aux services
  - Administrateurs délégués, le cas échéant
- Politique de sécurité, notamment gestion du firewall et du proxy

Chapitre

2

Installation et démarrage

À l'issue de ce chapitre, vous saurez comment démarrer l'Extended Communication Server et accéder à l'interface graphique d'administration.

2.1 Introduction

Deux options s'offrent à vous lorsque vous accédez pour la première fois à l'interface d'administration :

- Accès direct, le serveur étant équipé d'un écran, d'un clavier et d'une souris
- Accès depuis un PC local connecté au serveur

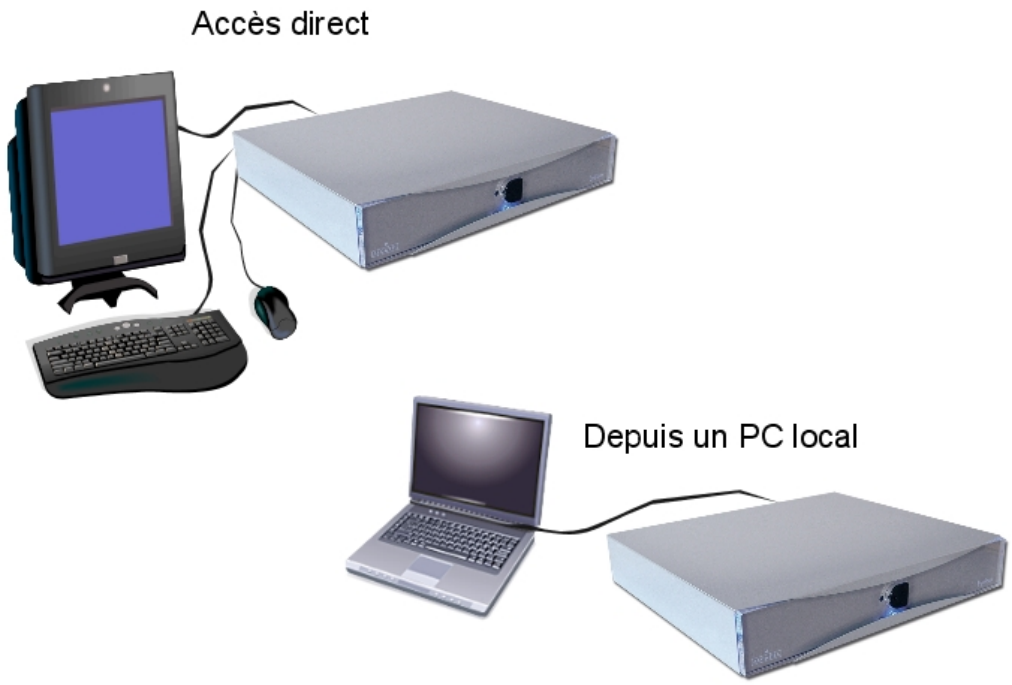


Figure 2.1 : Accès direct ou depuis un PC local

2.2 Démarrage via l'accès direct

Pour démarrer l'Extended Communication Server et accéder directement à son interface d'administration :

1. Déballez le serveur.
2. Branchez le câble d'alimentation.
3. Branchez un écran, un clavier et une souris sur le serveur.
   Le serveur dispose d'un port VGA pour l'écran et de ports PS/2 ou USB pour le clavier et la souris.

4. Allumez le serveur.
   Le noyau Linux démarre.
5. À l'invite de connexion :
   - Saisissez l'identifiant par défaut : `superadmin`
   - Saisissez le mot de passe par défaut : `%rV&A1uc`
   - Cliquez sur **VALIDER**.

   Le navigateur Web intégré s'ouvre.
6. Un message vous avertit que vous allez utiliser une session sécurisée. Cliquez sur oui pour continuer.

Security Alert
Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.
The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certifying authority.
The security certificate date is valid.
The security certificate has a valid name matching the name of the page you are trying to view.
Do you want to proceed?
Yes
No
View Certificate

7. Une boîte de dialogue de connexion s'affiche.
   - Saisissez l'identifiant par défaut : `superadmin`
   - Saisissez le mot de passe par défaut : `%rV&A1uc`
   - Cliquez sur **VALIDER**.

Vous avez désormais accès à l'interface d'administration.

2.3 Démarrage à partir d'un PC local

Pour démarrer l'Extended Communication Server à partir d'un PC local :

1. Déballez le serveur.
2. Branchez le câble d'alimentation.
3. Allumez le serveur.
4. À l'aide d'un câble croisé Ethernet, reliez le PC local à l'interface Ethernet LAN1 (eth0) du serveur.

   Note 1 :
   Il est également possible d'utiliser un câble Ethernet droit lorsque le PC est équipé d'un port Ethernet à détection automatique.

   Note 2 :
   Les plates-formes Compact et Premium proposent trois interfaces Ethernet. Le port Ethernet LAN1 (eth0) correspond au port Ethernet situé le plus à gauche sur le fond de panier.

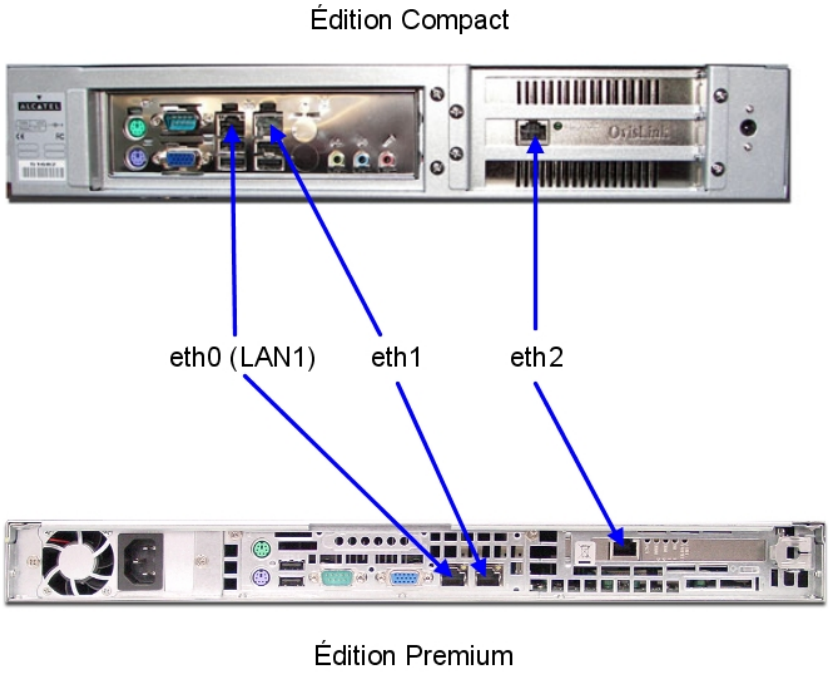


Figure 2.3 : Emplacement des ports Ethernet

5. Vérifiez que les paramètres réseau du PC sont compatibles avec les paramètres par défaut du serveur.
   Par défaut, le serveur est paramétré comme suit :
   - Adresse IP : **192.168.92.1**
   - Masque réseau : **255.255.255.0**
   - Protocole DHCP (Dynamic Host Configuration Protocol) désactivé

   Plage d'adresses autorisées : 192.168.92.2 à 192.168.92.254
6. Saisissez l'adresse `https://192.168.92.1` dans un navigateur Web standard.
7. Un message vous avertit que vous allez utiliser une session sécurisée. Cliquez sur oui pour continuer.

Security Alert
Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.
The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certifying authority.
The security certificate date is valid.
The security certificate has a valid name matching the name of the page you are trying to view.
Do you want to proceed?
Yes
No
View Certificate

8. Une boîte de dialogue de connexion s'affiche.
   - Saisissez l'identifiant par défaut : `superadmin`
   - Saisissez le mot de passe par défaut : `%rV&A1uc`
   - Cliquez sur **VALIDER**.

Vous avez désormais accès à l'interface d'administration.

2.4 Accès limité à l'interface d'administration

La première fois que vous démarrez l'Extended Communication Server et ouvrez une session d'administration, la majorité des menus est inaccessible car le pack logiciel est verrouillé.

Un guide de démarrage rapide particulièrement utile apparaît sur la gauche. Il vous servira au cours des premières étapes de la configuration du serveur, notamment pour sélectionner la langue du système et déverrouiller le pack logiciel à l'aide du numéro de licence du produit (voir chapitres suivants). Vous pouvez utiliser le guide de démarrage rapide en complément du présent document et le fermer lorsque vous n'en avez plus besoin. Pour le rouvrir ultérieurement, il vous suffit de cliquer sur l'icône en forme de point d'interrogation située dans la bannière supérieure du panneau de gauche.

Extended
Communication Server
Guide Rapide
Bienvenue dans le guide de démarrage rapide.
Mise en route
1. Configurez la langue de l'interface : Choix de la langue de votre interface.
2. Entrez la licence du produit ici : Packs & licences.
3. Réglez l'heure du système: Heure système.
Réseau
1. Si nécessaire, changez l'adresse IP de l'interface réseau LAN1 : Connexions Réseau. (n'oubliez pas de reconfigurer votre poste client).
2. Définissez le nom de votre Appliance ainsi que les serveurs de résolution de noms que vous souhaitez utiliser : Paramètres Réseau Généraux.

Figure 2.5 : Guide de démarrage rapide

Chapitre

3

Déverrouillage du pack logiciel

À l'issue de ce chapitre, vous saurez comment déverrouiller le pack logiciel de l'interface d'administration. Vous pourrez alors accéder à l'intégralité des menus d'administration.

3.1 Principes

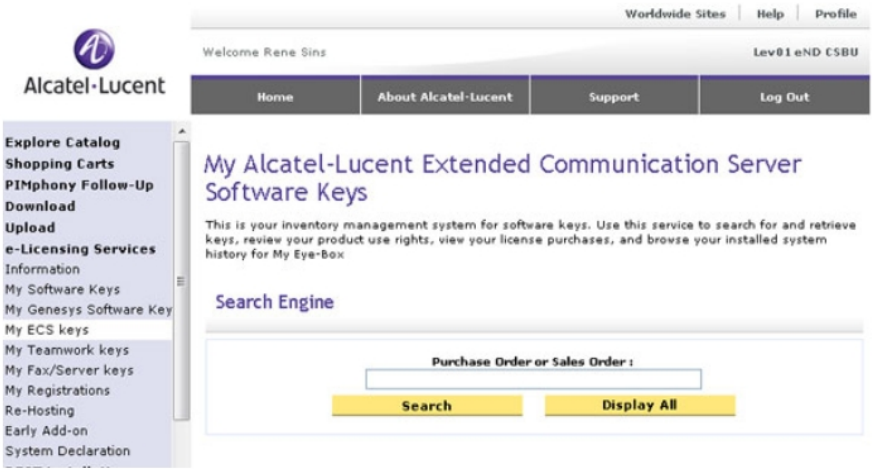
L'activation de la licence complète s'articule autour de deux étapes :

1. **Déverrouillage du pack logiciel**. Cette opération est traitée dans le présent chapitre. Le pack logiciel est alors déverrouillé pour 31 jours. Pendant cette durée limitée, aussi appelée période d'essai, l'ensemble des fonctions et des services est disponible.
2. **Activation de la licence**. Vous pouvez effectuer cette tâche immédiatement après avoir déverrouillé le pack logiciel, ou ultérieurement, mais dans tous les cas dans la période d'essai des 31 jours.
   . Il est plus facile d'effectuer cette tâche après que l'accès Internet a été activé. La licence peut ensuite être activée en ligne, en un simple clic. Sinon, la clé d'activation doit être saisie manuellement. Une fois la licence activée, l'ensemble des fonctions et des services est disponible indéfiniment.

3.2 Déverrouillage du pack logiciel

Pour déverrouiller le pack logiciel :

1. Vous devez d'abord vous procurer la clé logiciel du produit, également appelée numéro de licence. Pour ce faire, accédez au site Web Alcatel-Lucent Business Partner (https://www.businesspartner.alcatel-lucent.com/) et naviguez jusqu'à la page suivante : **ONLINE SERVICES > eBuy > e-Licenses Services > My ECS Keys**



2. Une fois que vous avez obtenu la clé logiciel, ouvrez l'interface d'administration et sélectionnez le menu **Gestion des services > Licences & Versions > Packs & licences**.
3. Sélectionnez l'onglet **Nouveau pack**.
4. Dans le champ **Clé d'activation ou Numéro de licence**, saisissez la clé logiciel.

5. Cliquez sur **VALIDER**.

Une fois le pack logiciel déverrouillé, des informations sur la licence apparaissent en bas du panneau, notamment le nombre de jours restants avant la fin de la période d'essai. N'oubliez pas d'activer la licence du produit dans le délai imparti.

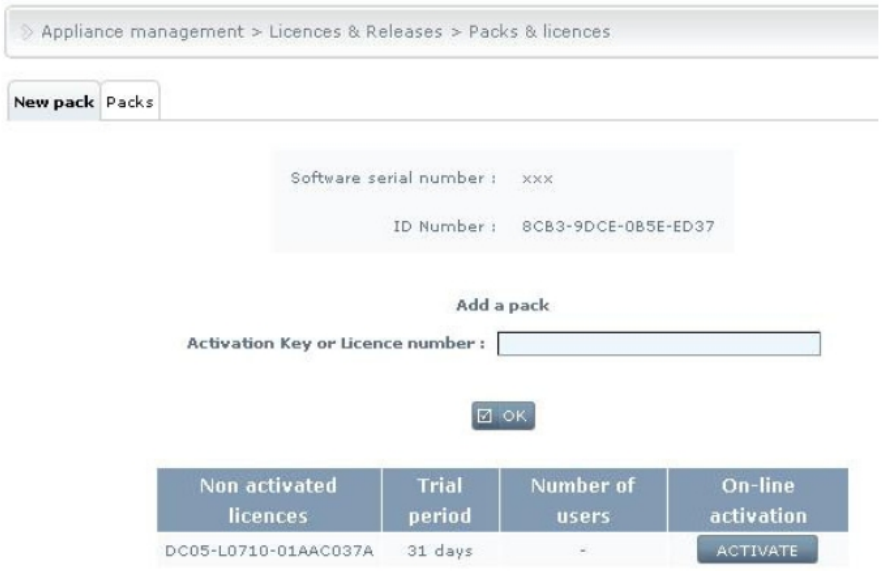


Figure 3.2 : Pack logiciel déverrouillé

Chapitre

4

Configuration du réseau

À l'issue de ce chapitre, vous saurez comment installer l'Extended Communication Server sur le réseau du client et accéder à Internet depuis l'interface d'administration.

4.1 Principes

Grâce à ses trois interfaces réseau et un ensemble exhaustif de paramètres de configuration, l'Extended Communication Server peut être installé sur n'importe quelle architecture de réseau.

Ce document n'a cependant pas pour but de décrire l'intégralité des architectures possibles. Son objectif est de vous présenter les principes fondamentaux et de fournir des exemples utiles illustrant les situations les plus courantes.

L'exemple ci-dessous explique comment installer l'Extended Communication Server dans une topologie de réseau standard :

- Le LAN (Local Area Network) est relié à l'interface eth0 (LAN1).
- Le réseau Internet est relié à l'interface eth1.
- Le DMZ (Demilitarized Zone) est relié à l'interface eth2. Un DMZ est un sous-réseau du LAN qui intègre les services externes accessibles depuis Internet, comme un serveur Web ou un serveur FTP, et facilite la gestion de la sécurité.

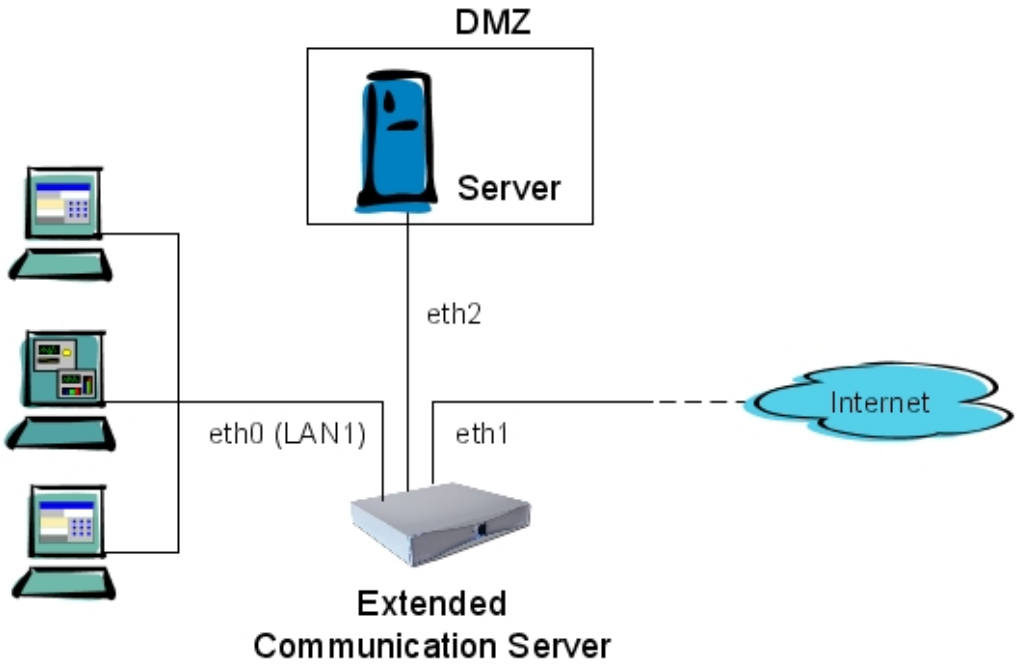


Figure 4.1 : Topologie de réseau standard

Ce chapitre décrit, dans l'ordre suivant, les principaux sous-menus **Gestion des services > Réseau** que vous serez amené à utiliser :

1. **Paramètres Réseau Généraux**
2. **Connexions Réseau**. Une fois configurées, les connexions réseau vous permettent d'accéder à Internet depuis l'interface d'administration (sauf si un proxy distant contrôle l'accès à Internet, comme expliqué dans la remarque suivante).
3. **DHCP**. Lorsque le service DHCP (Dynamic Host Configuration Protocol) est activé, vous pouvez accéder à l'interface d'administration et au Bureau Virtuel depuis n'importe quelle station de travail appartenant au LAN. Il est également possible d'affecter une adresse IP statique à chaque machine du LAN.

Note :

*Le sous-menu **Proxy distant** fait l'objet d'une section supplémentaire. Respectez les instructions fournies dans cette dernière si un proxy distant contrôle l'accès à Internet (dans les grandes entreprises généralement).*

4.2 Paramètres Réseau Généraux

Pour définir les paramètres réseau généraux :

1. Sélectionnez le menu **Gestion des services > Réseau > Paramètres Réseau Généraux**. Le formulaire Paramètres Réseau Généraux s'affiche.
2. Dans le champ **Nom d'hôte de l'Appliance**, saisissez le nom identifiant le serveur sur le réseau. Vous pouvez utiliser le nom de votre choix.
3. Dans le champ **Nom de domaine de l'Appliance**, saisissez le nom du domaine auquel le serveur appartient (« monentreprise.fr », par exemple).

   Important :
   Ce nom sera repris dans de nombreux paramètres, tels que les adresses e-mail.
4. Si l'accès au WAN s'effectue à partir d'une adresse attribuée de manière dynamique ou via une connexion PPPoE, les premier et deuxième serveurs de résolution de noms sont renseignés automatiquement.
   Dans le cas contraire, vous devez les définir manuellement :
   - Dans le champ **Premier serveur de résolution de noms**, saisissez l'adresse du serveur DNS (Domain Name System) fournie par le FAI (Fournisseur d'accès Internet).
   - Dans le champ **Deuxième serveur de résolution de noms**, saisissez l'adresse du deuxième serveur DNS fournie par le FAI (facultatif).
5. Cliquez sur **VALIDER**.

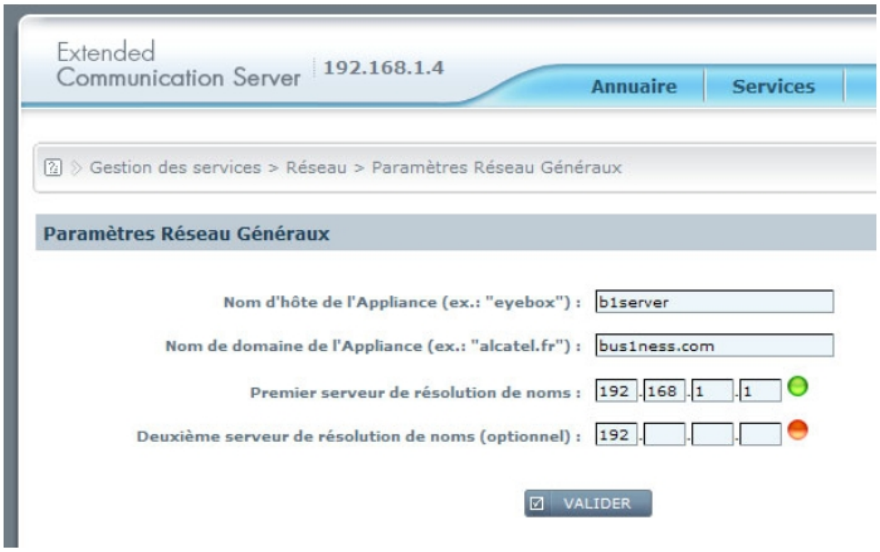


Figure 4.2 : Définition des paramètres réseau généraux

4.3 Connexions réseau

4.3.1 Généralités sur la configuration des connexions réseau

4.3.1.1 Interfaces réseau

Les serveurs Compact et Premium intègrent chacun trois interfaces réseau. Selon la version et l'édition du serveur, ces interfaces sont identifiées ou non par une étiquette sur le fond de panier.

Dans tous les cas, dans ce document, le terme LAN1 fait référence à l'interface Ethernet eth0, qui correspond au port RJ-45 situé le plus à gauche sur le fond de panier. LAN1 est le nom par défaut du port eth0.

Les trois interfaces peuvent être utilisées sans distinction pour toute connexion réseau.

Lors du démarrage initial, seule l'interface LAN1 existe par défaut et propose une connexion Ethernet au LAN. Vous ne pouvez ni supprimer cette connexion, ni en modifier le type. En revanche, tous les autres paramètres sont modifiables.

4.3.1.2 Types de connexions réseau

Définissez le type de connexion réseau que vous souhaitez créer parmi les cinq options suivantes :

- WAN ADSL PPPoE
- LAN Ethernet
- Pont Ethernet
- LAN Ethernet DMZ

- Alias LAN Ethernet

Ces cinq options sont détaillées dans les sections suivantes.

4.3.1.3 *Liste des connexions réseau*

Pour accéder à la liste des connexions, sélectionnez le menu **Gestion des services > Réseau > Connexions Réseau**.

La liste des connexions existantes s'affiche.

À partir de cette liste, vous pouvez :

- créer une connexion en cliquant sur le bouton Ajouter

;
- configurer une connexion existante en cliquant sur le bouton de modification .

4.3.2 Connexion WAN ADSL PPPoE

Une connexion *WAN ADSL PPPoE* établit une liaison entre une zone privée et une zone publique.

Dans l'exemple ci-dessous, l'utilisateur accède à Internet via un modem ADSL externe. L'adresse IP eth1 est publique.

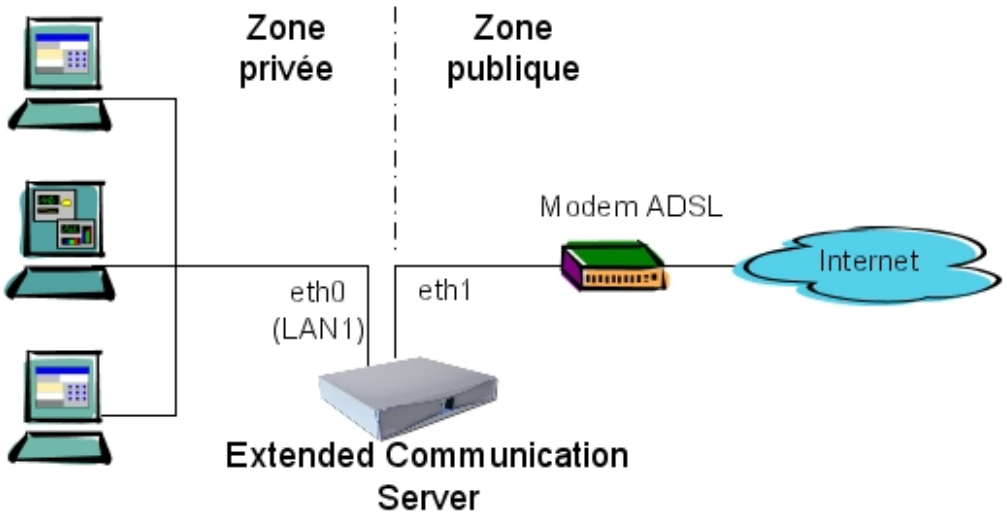


Figure 4.4 : Connexion WAN ADSL PPPoE sur eth1

Pour créer ou configurer une connexion *WAN ADSL PPPoE* :

1. Sélectionnez le menu **Gestion des services > Réseau > Connexions Réseau**. La liste des connexions s'affiche.
2. Si vous créez une connexion :
   a. Cliquez sur **Ajouter**.
   b. Sélectionnez l'option *WAN ADSL PPPoE*.
   c. Cliquez sur **VALIDER**.
   Sinon, si vous modifiez une connexion *WAN ADSL PPPoE* existante :
   a. Sélectionnez l'option *WAN ADSL PPPoE*.
   b. Cliquez sur le bouton de modification .
3. Saisissez le nom de la connexion dans le formulaire qui s'affiche. Choisissez un nom qui identifie clairement la connexion.
4. Le FAI peut configurer la connexion WAN de façon dynamique.
   Lorsque cette connexion n'est pas automatiquement configurée :
   a. Saisissez les paramètres PPPoE fournis par le FAI (identifiant, mot de passe et mot de passe de confirmation).
   b. Précisez si vous souhaitez utiliser les adresses des serveurs DNS qui ont été fournies par le FAI (recommandé).
5. Sélectionnez l'interface Ethernet (eth1/eth2, si proposé).
6. Sélectionnez **Oui** pour activer l'interface.
7. Validez les paramètres en cliquant sur **VALIDER**.

4.3.3 Connexion LAN Ethernet

Au sein de la zone privée, les interfaces réseau doivent être de type *LAN Ethernet*. Dans la figure ci-dessous, l'adresse IP de l'interface eth0 est privée, tandis que celle du routeur est publique. L'interface LAN1 correspond à une connexion *LAN Ethernet*.

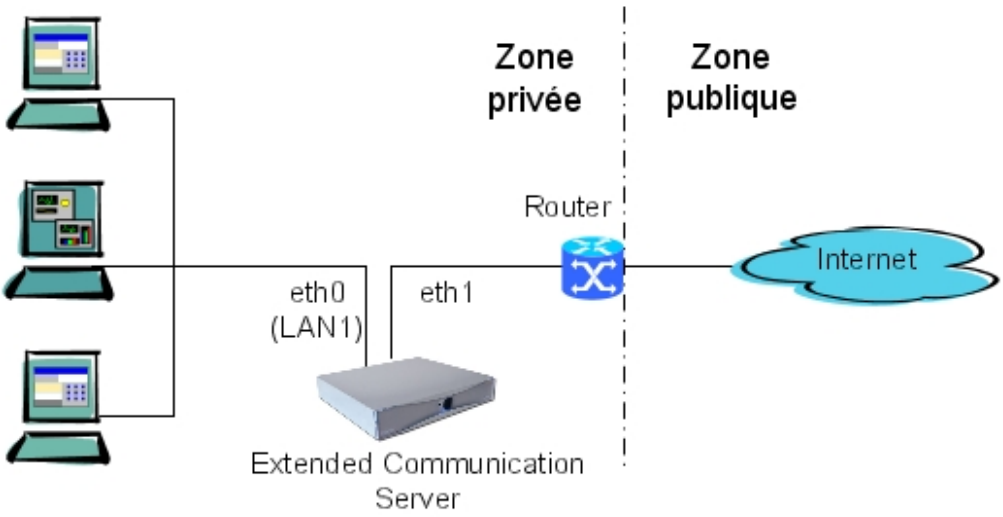


Figure 4.5 : Connexions LAN Ethernet sur eth0 et eth1

Pour créer ou configurer une connexion *LAN Ethernet* :

1. Sélectionnez le menu **Gestion des services > Réseau > Connexions Réseau**. La liste des connexions s'affiche.
2. Si vous créez une connexion :
   a. Cliquez sur **Ajouter**.
   b. Sélectionnez l'option *LAN Ethernet*.
   c. Cliquez sur **VALIDER**.
   Sinon, si vous modifiez une connexion *LAN Ethernet* existante :
   a. Sélectionnez l'option *LAN Ethernet*.
   b. Cliquez sur le bouton de modification .
3. Saisissez le nom de la connexion dans le formulaire qui s'affiche. Choisissez un nom qui identifie clairement la connexion.
4. Précisez si l'adresse IP de la connexion réseau est statique ou affectée par un serveur DHCP.
   Si elle est affectée par un serveur DHCP externe, ignorez l'étape suivante.
5. Définissez les paramètres de la connexion réseau :
   - Adresse IP de la connexion réseau
   - Masque de réseau ou préfixe équivalent
   - Adresse de la passerelle, en présence d'une passerelle externe (passerelle par défaut vers Internet uniquement)

Note :
Ne confondez pas la passerelle avec un routeur permettant d'accéder à un sous-réseau interne. Lorsque l'architecture n'intègre pas de passerelle externe, vous pouvez laisser le champ vide.

6. Sélectionnez l'interface Ethernet (ethx) lorsque plusieurs interfaces réseau sont proposées. Ce champ est en lecture seule dans les autres cas.
7. Sélectionnez **Oui** pour activer l'interface.
8. Validez les paramètres en cliquant sur **VALIDER**.

4.3.4 Connexion de pont Ethernet

Cette option permet de créer un pont Ethernet entre deux interfaces et plus qui, une fois reliées, forment un sous-réseau.

Par exemple, vous pouvez établir un pont entre une interface Wi-Fi et une interface LAN1 en vue d'étendre le réseau local aux périphériques Wi-Fi (voir figure ci-dessous).

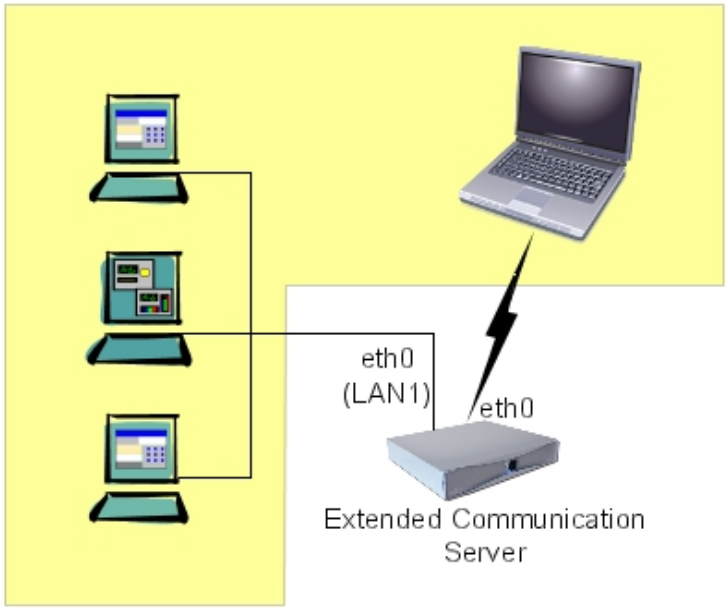


Figure 4.6 : Connexion de type pont entre une interface Wi-Fi et une interface LAN1

Pour créer ou configurer une connexion de type *pont Ethernet* :

1. Sélectionnez le menu **Gestion des services > Réseau > Connexions Réseau**. La liste des connexions s'affiche.
2. Si vous créez une connexion :
   a. Cliquez sur **Ajouter**.
   b. Sélectionnez l'option *Pont Ethernet*.
   c. Cliquez sur **VALIDER**.
   Sinon, si vous modifiez une connexion de type *pont Ethernet* existante :

a. Sélectionnez l'option *Pont Ethernet*.

b. Cliquez sur le bouton de modification .

3. Saisissez le nom de la connexion dans le formulaire qui s'affiche. Choisissez un nom qui identifie clairement la connexion.
4. Si le pont n'est pas relié à l'interface LAN1, définissez les paramètres IP du pont Ethernet. Dans le cas contraire, cochez la case LAN1. Les paramètres IP sont alors automatiquement renseignés.
5. Sélectionnez les interfaces à relier par le pont Ethernet.
6. Sélectionnez **Oui** pour activer l'interface.
7. Validez les paramètres en cliquant sur **VALIDER**.

4.3.5 Connexion LAN Ethernet DMZ

Une connexion LAN Ethernet DMZ permet de relier un réseau local démilitarisé qui devient accessible via Internet, comme illustré à la figure : Topologie de réseau standard .

Pour créer ou configurer une connexion *LAN Ethernet DMZ* :

1. Sélectionnez le menu **Gestion des services > Réseau > Connexions Réseau**. La liste des connexions s'affiche.
2. Si vous créez une connexion :

   a. Cliquez sur **Ajouter**.

   b. Sélectionnez l'option *LAN Ethernet DMZ*.

   c. Cliquez sur **VALIDER**.

   Sinon, si vous modifiez une connexion *LAN Ethernet DMZ* existante :

   a. Sélectionnez l'option *LAN Ethernet DMZ*.

   b. Cliquez sur le bouton de modification .
3. Saisissez le nom de la connexion dans le formulaire qui s'affiche. Choisissez un nom qui identifie clairement la connexion.
4. Définissez les paramètres de la connexion réseau :
   - Adresse IP de la connexion réseau
   - Masque de réseau ou préfixe équivalent
   - Adresse de la passerelle, le cas échéant
5. Sélectionnez l'interface Ethernet (ethx) lorsque plusieurs interfaces réseau sont proposées. Ce champ est en lecture seule dans les autres cas.
6. Sélectionnez **Oui** pour activer l'interface.
7. Validez les paramètres en cliquant sur **VALIDER**.

4.3.6 Connexion Alias LAN Ethernet

Une connexion Alias LAN Ethernet permet de créer une interface virtuelle à partir d'une interface existante. Vous pouvez ainsi affecter différentes adresses IP à une interface réseau physique.

Pour créer ou configurer une connexion *Alias LAN Ethernet* :

1. Sélectionnez le menu **Gestion des services > Réseau > Connexions Réseau**. La liste des connexions s'affiche.
2. Si vous créez une connexion :
   a. Cliquez sur **Ajouter**.
   b. Sélectionnez l'option *Alias LAN Ethernet*.
   c. Cliquez sur **VALIDER**.
   Sinon, si vous modifiez une connexion *Alias LAN Ethernet* existante :
   a. Sélectionnez l'option *Alias LAN Ethernet*.
   b. Cliquez sur le bouton de modification .
3. Saisissez le nom de la connexion dans le formulaire qui s'affiche. Choisissez un nom qui identifie clairement la connexion.
4. Définissez les paramètres de la connexion réseau :
   - Adresse IP de la connexion réseau
   - Masque de réseau ou préfixe équivalent
5. Sélectionnez l'interface Ethernet physique (ethx) lorsque plusieurs interfaces réseau sont proposées. Ce champ est en lecture seule dans les autres cas.
6. Sélectionnez **Oui** pour activer l'interface.
7. Validez les paramètres en cliquant sur **VALIDER**.

4.4 Service DHCP

Lorsque le service DHCP est activé sur une interface réseau donnée, l'Extended Communication Server joue le rôle de serveur DHCP pour tous les périphériques appartenant au sous-réseau correspondant. Ainsi, chaque fois que le serveur détecte un nouveau périphérique client, il lui affecte une adresse IP dynamique, vous évitant ainsi d'avoir à gérer manuellement des adresses statiques.

Dans l'exemple ci-dessous, le service DHCP est activé sur l'interface LAN1.

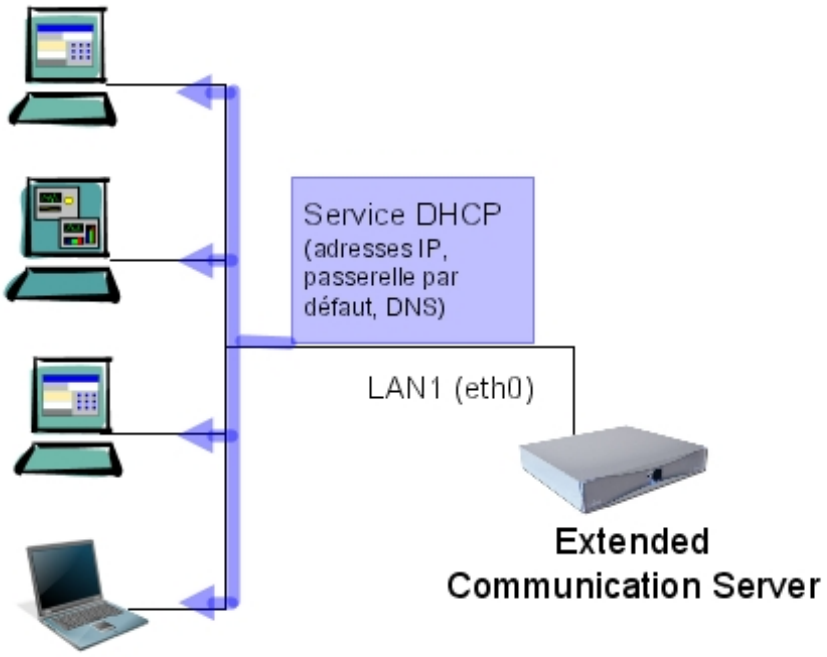


Figure 4.7 : Service DHCP activé sur interface LAN1

Le service DHCP est accessible via le sous-menu **Gestion des services > Réseau > DHCP**. Ce sous-menu se compose de trois onglets, lesquels sont décrits dans les sections suivantes.

Note :
*Une fois le service DHCP configuré, sélectionnez l'option **Actif** pour l'activer.*

4.4.1 Configuration globale

Pour configurer le service DHCP :

1. Sélectionnez l'onglet **Configuration globale**.
2. Sélectionnez la connexion réseau appropriée.
3. Précisez la durée du bail DHCP, c'est-à-dire la période de validité des adresses IP affectées.
4. Indiquez la plage d'adresses IP réservées au service DHCP (début et fin de plage).
5. Saisissez l'adresse IP de la passerelle (adresse de l'interface réseau concernée, en général).
6. Saisissez les adresses IP des serveurs DNS :
   - Lorsque le service DNS est activé, saisissez l'adresse de l'interface réseau concernée.
   - Lorsque le service DNS est désactivé, saisissez les adresses des serveurs DNS qui ont été fournies par le FAI.
7. Saisissez les adresses IP des serveurs WINS (facultatif). Le service WINS (Windows

Internet Name Service) permet le partage du réseau Windows.

- Lorsque le service DNS est activé, saisissez l'adresse de l'interface réseau concernée.
- Lorsque le service DNS est désactivé, saisissez les adresses des serveurs DNS qui ont été fournies par le FAI.

8. Cliquez sur **VALIDER**.

4.4.2 Machines déclarées

Utilisez l'onglet **Machines déclarées** pour définir des comportements particuliers dans le cadre du service DHCP, par exemple :

- Une machine requiert une adresse IP statique (serveur ou imprimante, par exemple).
- Vous souhaitez limiter le service DHCP à une liste donnée de machines (afin d'empêcher les visiteurs équipés d'ordinateurs portables de se connecter au réseau local, par exemple).

Pour déclarer une machine :

1. Sélectionnez l'onglet **Machines déclarées**.
2. Sélectionnez la connexion réseau appropriée.
3. Saisissez un nom qui identifie clairement la machine sur le réseau.
4. Saisissez son adresse MAC. L'adresse MAC (Media Access Control) constitue un identifiant unique associé à la carte réseau d'une machine.
5. Précisez si l'adresse IP de la machine est statique ou dynamique (affectée par le serveur DHCP).
6. Si la machine a une adresse IP statique, saisissez cette dernière. L'adresse doit appartenir au réseau concerné et ne doit pas figurer dans la plage d'adresses IP réservées au service DHCP.
7. Cliquez sur **VALIDER**.

4.4.3 Baux DHCP

L'onglet **Baux DHCP** est fourni à titre d'information seulement. Il dresse la liste des baux DHCP qui ont été affectés aux machines.

4.5 Proxy distant

Certaines entreprises de grande taille contrôlent l'accès à Internet au moyen de leur propre proxy (au lieu d'un proxy hébergé par l'Extended Communication Server). Dans ce cas, vous devez configurer l'accès au proxy distant de manière que le serveur puisse se connecter à Internet (obligatoire pour la fonction de mise à jour automatique).

Pour accéder à Internet via un proxy distant :

1. Sélectionnez le menu **Gestion des services > Réseau > Proxy distant**.
   Le formulaire de configuration de l'accès au proxy distant s'affiche.
2. Sélectionnez l'option **La connexion internet passe par le proxy distant suivant**.
3. Définissez les paramètres d'accès en fonction de la configuration du proxy distant :
   - Adresse IP du proxy distant

- Port d'écoute
- Authentification par login et mot de passe, le cas échéant

4. Cliquez sur **VALIDER**.

Chapitre

5

Enregistrement, activation et mises à jour

À l'issue de ce chapitre, vous saurez comment accéder au support technique en ligne de l'Extended Communication Server pour activer la licence complète et mettre à jour les packs logiciels.

5.1 Généralités

Maintenant que vous avez accès à Internet depuis l'interface d'administration, vous pouvez activer définitivement la licence et mettre à jour les packs logiciels. Cette mise à niveau vous offre la garantie d'un logiciel bénéficiant des dernières avancées techniques. Tout dysfonctionnement peut aussi être corrigé.

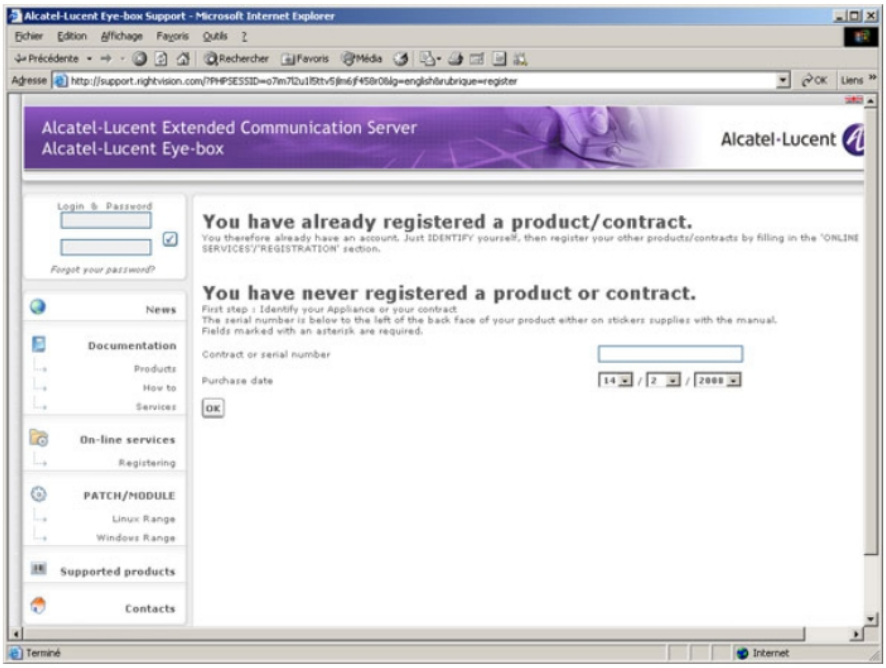
Vous devez d'abord enregistrer votre produit Extended Communication Server avant d'activer la licence et de mettre à jour les logiciels.

5.2 Enregistrement et génération de la clé d'activation

L'enregistrement du produit est obligatoire pour avoir accès au support technique.

Pour enregistrer le produit et générer la clé d'activation :

1. Depuis n'importe quel PC connecté à Internet, accédez au site Web d'assistance de l'Extended Communication Server, à l'adresse suivante : http://support.rightvision.com/.



2. Si vous disposez déjà d'un compte utilisateur :
   a. Saisissez vos login et mot de passe, puis cliquez sur **OK**.
   b. Sélectionnez **On-line services > Registering**.
   c. Suivez les instructions qui apparaissent à l'écran.

Si vous n'avez pas de compte utilisateur :

a. Sélectionnez **On-line services > Registering**.

b. Saisissez le numéro de contrat ou le numéro de série de l'Extended Communication Server, puis cliquez sur **OK**. Le numéro de série figure sur une étiquette située sur le châssis du serveur.

c. Suivez les instructions pour créer votre compte utilisateur.

d. Une fois le compte créé, utilisez-le pour vous connecter.

3. Sélectionnez **On-line services > Activation of my licenses**.
4. Saisissez le numéro d'ID requis. Vous pouvez trouver ce numéro d'ID dans l'interface d'administration, depuis le menu **Gestion du boîtier > Licences & Versions > Versions Logiciel**.

Gestion du boîtier > Licences & Versions > Versions Logiciel
Versions Logiciel
Liste des RPMS installés
Numéro de série logiciel : R07163MN4EU0006
Numéro d'ID : 5108-8C02-D270-717C
Build Number : 712401314005EU
Version : 4005
VALIDER

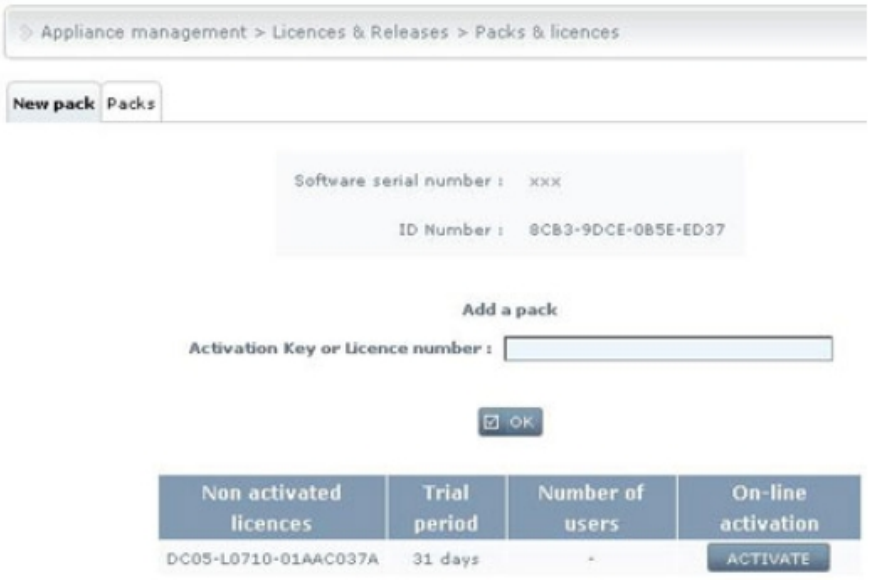
5. Cliquez sur le bouton .
6. Saisissez le numéro de la licence.
   Une clé d'activation est alors générée, laquelle vous permet d'activer la licence depuis l'interface d'administration. Pour activer la licence manuellement, copiez la clé d'activation et collez-la dans un fichier texte.

5.3 Activation de la licence

La licence doit être activée avant l'issue de la période d'essai de 31 jours.

Pour activer la licence :

1. Sélectionnez le menu **Gestion du boîtier > Licences & Versions > Packs & licences**.
2. Sélectionnez l'onglet **Nouveau pack**.



3. Deux méthodes d'activation vous sont proposées :
   - Si Internet est accessible, effectuez l'activation en ligne en cliquant sur le bouton **ACTIVER**.
   - Si Internet n'est pas accessible, utilisez la clé d'activation que vous avez préalablement enregistrée dans un fichier texte (voir § Enregistrement et génération de la clé d'activation).
     Copiez cette clé, collez-la dans le champ **Clé d'activation ou Numéro de licence**, puis cliquez sur **VALIDER**.

Une fois la licence activée, l'onglet **Nouveau pack** affiche un historique des licences.

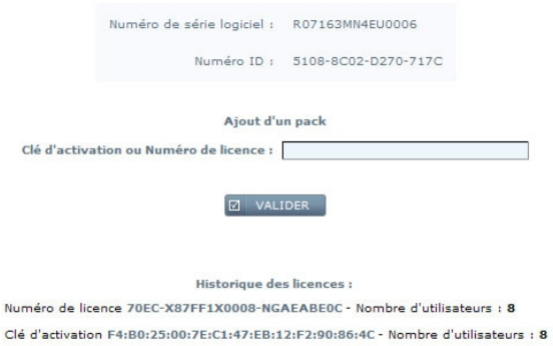

Numéro de série logiciel : R07163MN4EU0006
Numéro ID : 5108-8C02-D270-717C
Ajout d'un pack
Clé d'activation ou Numéro de licence :
VALIDER
Historique des licences :
Numéro de licence 70EC-X87FF1X0008-NGAEABE0C - Nombre d'utilisateurs : 8
Clé d'activation F4:B0:25:00:7E:C1:47:EB:12:F2:90:86:4C - Nombre d'utilisateurs : 8

Figure 5.4 : Historique des licences après activation du logiciel

5.4 Mises à jour logicielles

Par défaut, le système de l'Extended Communication Server est mis à jour chaque semaine via Internet.

Note 1 :

Certains packs logiciels ne sont pas mis à jour automatiquement. Cette opération doit être réalisée manuellement.

Nous vous recommandons :

- de toujours activer la mise à jour automatique ;
- d'effectuer une mise à jour manuelle après l'installation ou après une réinitialisation du serveur.

Pour effectuer une mise à jour manuelle :

1. Sélectionnez le menu **Gestion du boîtier > Mises à jour du boîtier > Mise à jour par le Web**.
2. Cliquez sur le bouton **Mise à jour manuelle**.
3. Suivez les instructions qui apparaissent à l'écran.

Note 2 :

Certaines mises à jour exceptionnelles peuvent nécessiter l'emploi d'un CD-ROM ou d'un périphérique USB. Dans ce cas, utilisez le menu ***Gestion du boîtier > Mises à jour du boîtier > Mise à jour par CD-ROM / USB*** *et suivez les instructions qui apparaissent à l'écran.*

Chapitre

6

Gestion des utilisateurs

À l'issue de ce chapitre, vous aurez un aperçu de la gestion des groupes d'utilisateurs et des comptes utilisateurs. Reportez-vous à l'aide en ligne pour plus de détails.

6.1 Généralités

La répartition des utilisateurs au sein de groupes d'utilisateurs doit refléter la structure de l'entreprise, répondre aux besoins de cette dernière et anticiper les évolutions futures. Nous vous recommandons de planifier cette répartition avant même de créer les groupes et les comptes.

L'administrateur de l'Extended Communication Server gère deux types de groupes d'utilisateurs :

- **Groupes standard**
  Chaque utilisateur est membre d'un groupe ou sous-groupe standard. Vous devez d'abord créer un groupe ou un sous-groupe standard avant de créer les comptes utilisateurs associés.
- **Groupes virtuels**. Un utilisateur peut appartenir à des groupes virtuels, mais ce n'est pas une obligation. Vous pouvez à tout moment créer des groupes virtuels et leur affecter n'importe quel compte utilisateur existant.

L'exemple ci-dessous explique comment utiliser les groupes standard et virtuels pour décrire une entreprise.

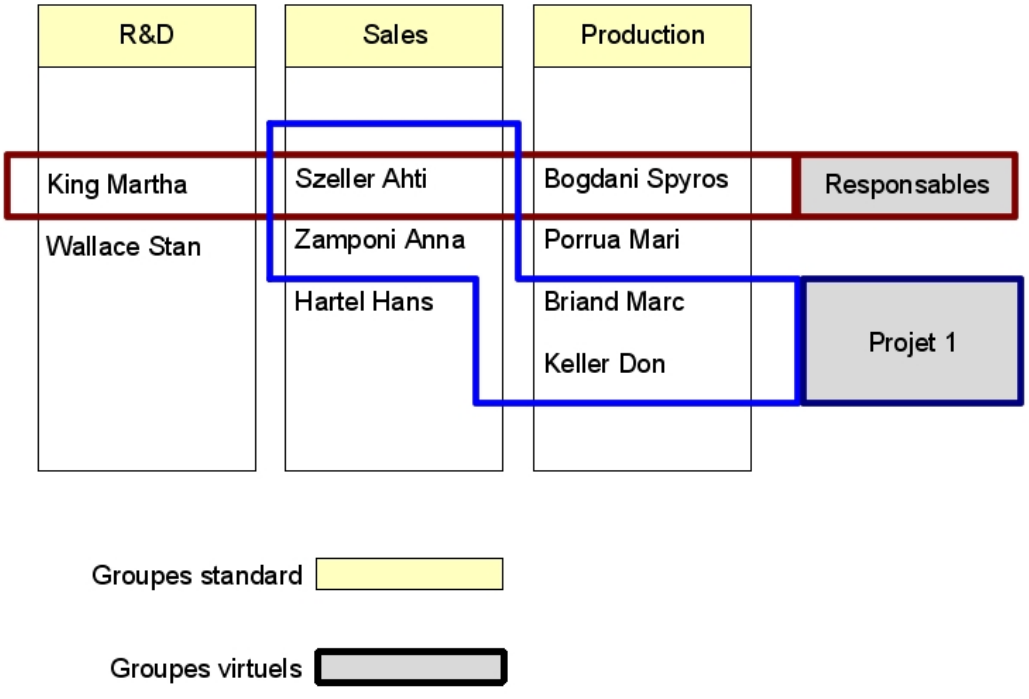


Figure 6.1 : Exemple de structure

6.2 Gestion des groupes d'utilisateurs et des comptes utilisateurs

La gestion des groupes d'utilisateurs et comptes utilisateurs s'effectue à partir du menu **Annuaire > Comptes utilisateurs**.

Le formulaire qui s'affiche se décompose en deux parties :

- Zone des groupes dans la partie gauche (liste des groupes d'utilisateurs et boutons de gestion associés)
- Zone des utilisateurs dans la partie droite (liste des comptes utilisateurs et boutons de gestion associés)

Figure 6.2 : Zone des groupes et zone des utilisateurs

6.2.1 Création de groupes d'utilisateurs

Pour créer un groupe d'utilisateurs :

1. Si vous souhaitez créer un groupe standard, sélectionnez le groupe parent (groupe racine ou autre groupe existant) dans la partie gauche du formulaire.
2. Cliquez sur **Ajouter**.
3. Saisissez le nom du groupe.
4. Précisez s'il s'agit d'un groupe **standard** ou **virtuel**.
5. Ajoutez une description si nécessaire.
6. Saisissez l'adresse e-mail du groupe. Tous les utilisateurs du groupe recevront les e-mails envoyés à cette adresse.
7. Cliquez sur **VALIDER**.

Une fois le groupe créé :

- Dans le cas d'un groupe standard , la prochaine étape consiste à créer les comptes utilisateurs associés.
- Dans le cas d'un groupe virtuel , vous pouvez ajouter des comptes utilisateurs qui existent déjà. Les utilisateurs d'un groupe virtuel sont en fait considérés comme des

personnes *invitées* à faire partie de ce groupe.

6.2.2 Création de comptes utilisateurs

Note 1 :
Vous devez avoir créé un groupe ou un sous-groupe standard avant de créer les comptes utilisateurs associés.

Pour créer un compte utilisateur :

1. Dans la partie gauche du formulaire, sélectionnez le groupe ou sous-groupe standard dont l'utilisateur sera membre.
2. Dans la partie droite du formulaire, cliquez sur **Ajouter**.
3. Saisissez les informations relatives à l'utilisateur (nom, prénom, etc.). Un astérisque ***** apparaît devant les champs obligatoires.
4. Indiquez si le compte utilisateur est actif ou non. Il est actif par défaut. Cette option permet de désactiver un compte utilisateur au lieu de le supprimer.
5. Vous pouvez éventuellement limiter l'espace réservé au compte utilisateur sur le disque.
6. Définissez les autorisations d'accès au FTP et au Web.
7. Définissez les droits de l'utilisateur, le cas échéant (voir section suivante).
8. Affectez des adresses e-mail à l'utilisateur.
9. Si nécessaire, autorisez l'utilisateur à envoyer et recevoir des e-mails gérés par un serveur distant (messagerie distante).
10. Cliquez sur **VALIDER**.

Note 2 :
L'interface d'administration vous permet également d'importer des comptes utilisateurs au format CSV (Comma-separated Values). Pour ce faire, sélectionnez le menu ***Annuaire > Import/Export utilisateurs > Import utilisateurs (format csv)*** *et suivez les instructions fournies dans l'aide en ligne. Cette aide propose une description complète du format CSV, en plus d'autres informations.*

6.3 Droits des utilisateurs

Vous avez la possibilité d'affecter des rôles particuliers à certains utilisateurs :

- L'**administrateur délégué** (un par groupe d'utilisateurs) gère les comptes utilisateurs de son groupe ou d'un autre groupe. Cette personne peut ajouter, modifier, supprimer des comptes utilisateurs, et affecter certains droits d'accès aux services. L'administrateur délégué peut aussi être responsable des sites Web de l'entreprise, comme le site Intranet.
- Le **graphiste du Bureau Virtuel** gère la charte graphique du Bureau Virtuel (logo, couleurs, etc.).
- L'**administrateur des news** assure la diffusion des news auprès de tous les utilisateurs.
- L'**administrateur des news du groupe** assure la diffusion des news auprès de tous les utilisateurs du groupe.

Chapitre 6 *Gestion des utilisateurs*

Chapitre 7

Gestion de la sécurité

Ce chapitre présente les différentes fonctions de gestion de la sécurité des informations et de surveillance du trafic offertes par l'Extended Communication Server. Après l'avoir consulté, vous saurez comment planifier et mettre en œuvre les mesures visant à sécuriser les informations de l'entreprise.

7.1 Présentation

Pour la gestion de la sécurité, l'Extended Communication Server est doté :

- d'un serveur proxy interne,
- d'un firewall interne.

Le firewall est activé par défaut, contrairement au serveur proxy.

Note :

Nous vous recommandons de configurer et d'activer les services de proxy et de firewall.

En outre, pour une sécurité optimale du réseau, il est également conseillé d'utiliser les options suivantes de l'Extended Communication Server :

- ***Optenet**, pour un filtrage efficace des URL,*
- ***Kaspersky**, pour une protection anti-virus renforcée.*

7.2 Gestion du firewall

7.2.1 Généralités

Lorsqu'il est activé, le firewall permet de filtrer les flux de trafic entre les différentes interfaces réseau. Sa fonction principale consiste à séparer du trafic Internet les informations et ressources internes de l'entreprise.

La gestion du firewall vise à définir des **règles** autorisant ou interdisant l'accès d'un **service ou groupement de services** donné à un **flux** particulier.

7.2.1.1 Flux de trafic

Un flux de trafic est défini par :

- deux points d'extrémité, l'interface LAN1 (reliée au LAN de l'entreprise) et l'interface réseau connectée à Internet par exemple,
- le sens du trafic, de l'interface LAN1 vers l'interface réseau connectée à Internet par exemple.

L'interface d'administration affiche automatiquement les flux de trafic existants, en fonction des interfaces réseau créées.

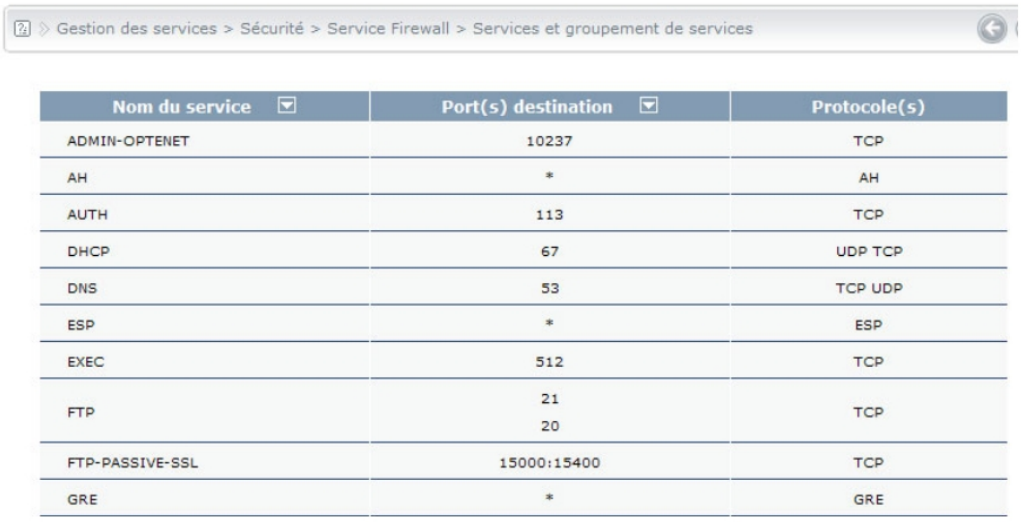
7.2.1.2 Services et groupements de services

Un service est défini par :

- un nom (généralement le nom du protocole de service, par exemple HTTP, mais toute valeur est autorisée),

- un numéro de port servant à identifier les applications émettrices et réceptrices (par exemple, le port 80 représente le service http),
- un protocole de transport (TCP - Transmission Control Protocol - ou UDP - User Datagram Protocol).

Une liste de services prédéfinis est mise à votre disposition. Pour y accéder, sélectionnez le menu **Gestion des services > Sécurité > Service Firewall > Services et groupement de services**, puis cliquez sur l'onglet **Services**. Vous avez la possibilité d'ajouter des services à la liste en fonction de vos besoins.



Nom du service	Port(s) destination	Protocole(s)
ADMIN-OPTENET	10237	TCP
AH	*	AH
AUTH	113	TCP
DHCP	67	UDP TCP
DNS	53	TCP UDP
ESP	*	ESP
EXEC	512	TCP
FTP	21 20	TCP
FTP-PASSIVE-SSL	15000:15400	TCP
GRE	*	GRE

Figure 7.1 : Liste des services disponibles

Pour faciliter la gestion du firewall, vous pouvez rassembler les services en groupements de services. Par exemple, vous utiliserez un groupement MAIL, contenant les services SMTP, POP et IMAP, pour autoriser ou interdire ces trois services en une seule opération.

Certains groupements de services sont prédéfinis. Utilisez l'onglet **Groupements de services** pour accéder aux groupements existants et ajouter vos propres groupements au besoin.

Gestion des services > Sécurité > Service Firewall > Services et groupement de services
Services
Groupements de services
Groupements de services
Nom du groupe :
CRÉER UN NOUVEAU GROUPE

Groupements de services	Services
FROM_OXO	OXO-DISCOVERY OXO-FTP-DATA
MAIL	IMAP POP SMTP

Figure 7.2 : Liste des groupements de services

7.2.1.3 Règles de firewall

L'interface d'administration propose deux méthodes d'accès aux règles existantes :

- Le menu **Configuration de base** contient les principales règles de protection du réseau, regroupées en flux principaux. Utilisez-le pour consulter les règles appliquées au firewall ou pour vos paramétrages de base.
- Le menu **Paramètres avancés** contient l'ensemble des flux disponibles, avec les règles associées. Utilisez-le pour vos besoins spécifiques.

Par défaut, aucun service n'est autorisé.

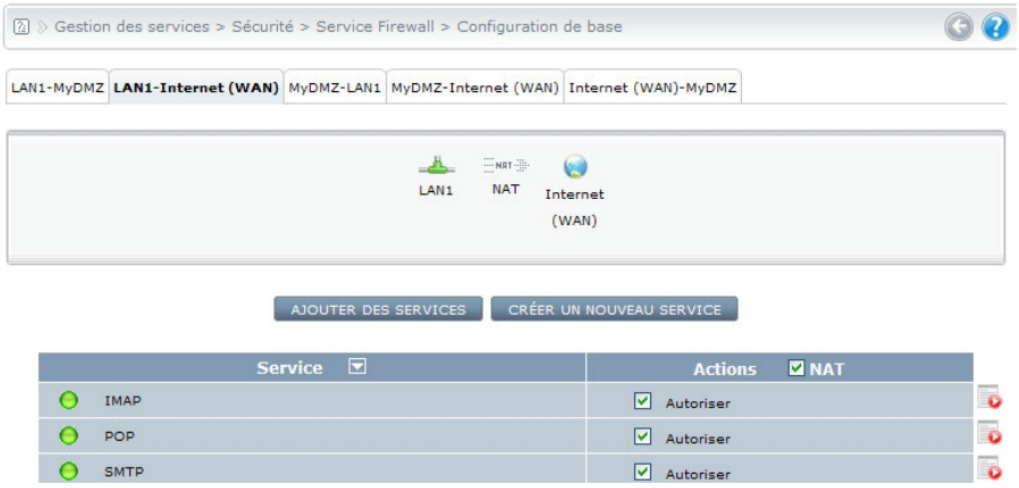


Figure 7.3 : Panneau à onglets Configuration de base

7.2.2 Paramètres avancés

L'Extended Communication Server crée automatiquement toutes les règles nécessaires à la gestion du firewall, en fonction des interfaces réseau que vous avez déclarées. Généralement, il vous suffit de modifier les règles préexistantes pour autoriser ou interdire un service donné sur un flux particulier.

Dans certains cas cependant, vous serez amené à créer manuellement des règles. Dans l'exemple ci-dessous, une partie du LAN est cachée derrière un routeur (du point de vue du serveur). Vous devez créer une règle autorisant les utilisateurs du sous-réseau à utiliser les services (service de messagerie, dans l'exemple).

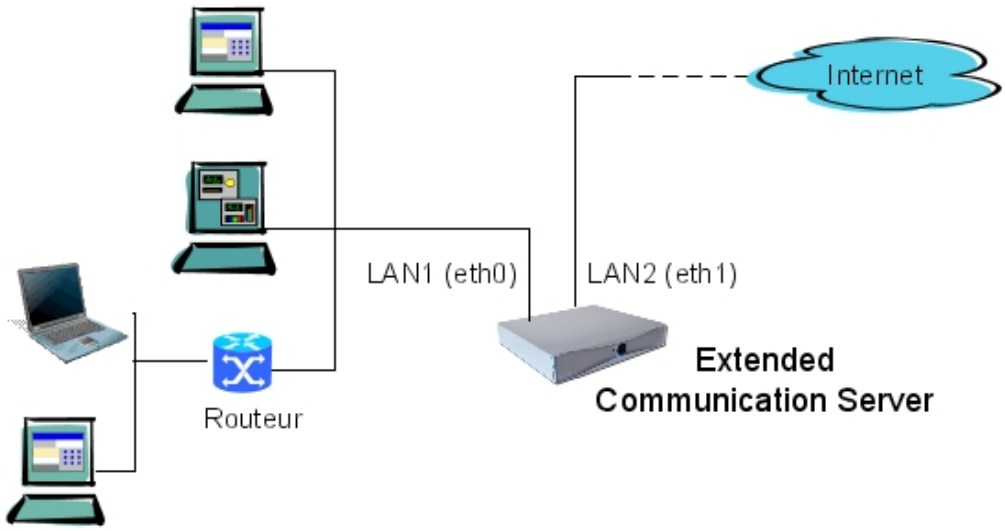
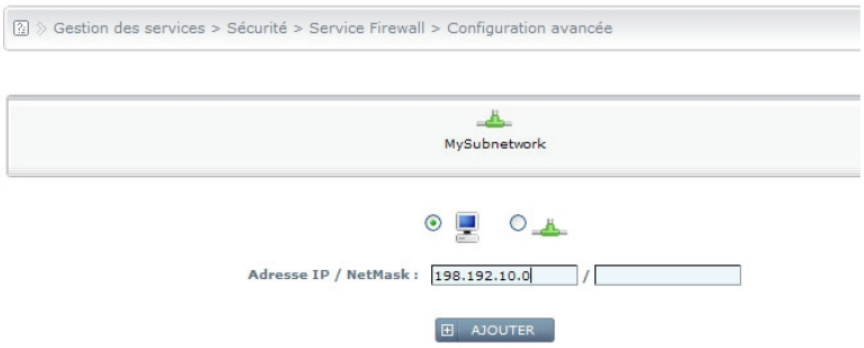


Figure 7.4 : LAN avec sous-réseau

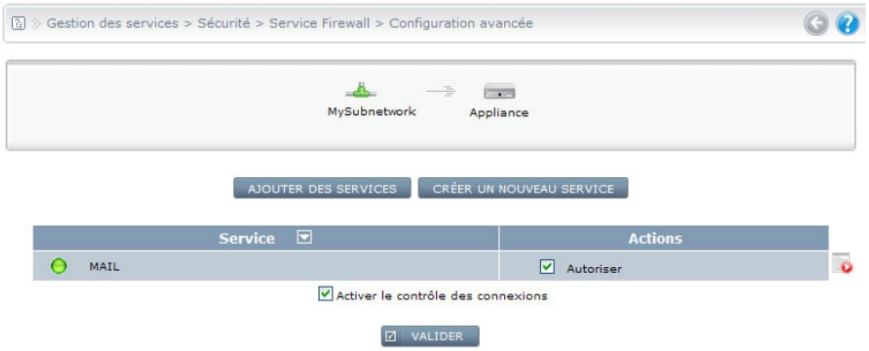
Pour créer une règle pour ce sous-réseau :

1. Sélectionnez le menu **Gestion des services > Sécurité > Firewall > Paramètres avancés**.
2. Sélectionnez l'onglet **Groupement de machines, Réseaux**.
3. Dans le champ **Nom du nouveau groupe ou réseau**, saisissez le nom du sous-réseau.
4. Cliquez sur **Créer**.
   Un formulaire de création s'affiche.



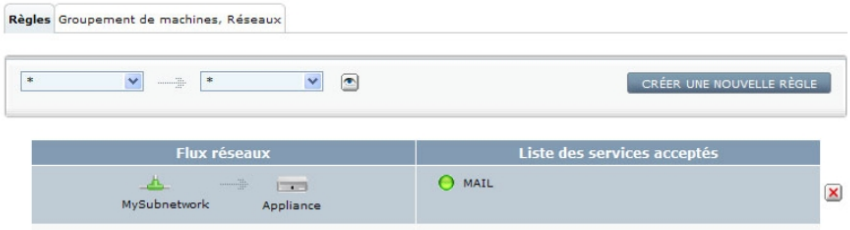
   a. Sélectionnez l'option correspondant au réseau.
   b. Saisissez l'adresse et le masque du réseau.
   c. Cliquez sur **OK**.
   Le nouvel élément est ajouté à la liste des machines et des réseaux.

5. Sélectionnez l'onglet **Règles**.
6. Sélectionnez le flux voulu (de *MySubnetwork* vers *Appliance*, dans le cas présent) à partir des listes déroulantes situées en haut du formulaire.
7. Cliquez sur **Créer une nouvelle règle**.
   Un formulaire de création de règle s'affiche.



   a. Sélectionnez un service ou un groupement de services dans ce formulaire (groupement de services MAIL, dans le cas présent). Vous pouvez éventuellement utiliser ce formulaire pour créer des services.
   b. Cliquez sur **Ajouter**.
   c. Cliquez sur **OK**.

   La règle apparaît désormais dans la liste.



Les trois protocoles des services du groupement MAIL, à savoir SMTP, POP et IMAP, sont

autorisés pour ce flux.

Note :

Une fois les règles du firewall définies, nous vous recommandons de les enregistrer à l'aide du menu ***Gestion des services > Sécurité > Firewall > Sauvegarde et restauration des règles****.*

7.3 Gestion du serveur proxy

7.3.1 Services proxy

Le serveur proxy est une application interne qui traite les requêtes Internet du poste client et fournit les services suivants :

- **Service de cache**. Lorsque ce service est actif, le serveur proxy conserve une copie en local de chaque requête du client. De cette manière, il peut répondre à une requête en renvoyant le contenu des requêtes précédentes, au lieu d'avoir à contacter les serveurs distants. En plus d'optimiser l'utilisation de la bande passante, ce service améliore les performances du système.
  Il fournit également des statistiques sur le trafic Web.
- **Contrôle d'accès au Web**. Le serveur proxy peut autoriser ou bloquer l'accès au Web pour chacun des utilisateurs.
- **Filtrage Web**. Le filtrage Web repose sur des black et white listes d'URL et de mots-clés qui interdisent ou autorisent l'accès à certains sites Web. Ces filtres s'appliquent à tous les utilisateurs ou à des groupes spécifiques d'utilisateurs.

Note :

Le navigateur Web du client doit être configuré pour envoyer le trafic Web vers le serveur proxy.

Important :

Lorsque vous utilisez un serveur proxy pour contrôler et filtrer le trafic Web, le firewall doit bloquer les flux http et https. De cette manière, le trafic Web est obligé de passer par le serveur proxy, condition sine qua non pour assurer un service de contrôle et de filtrage efficace.

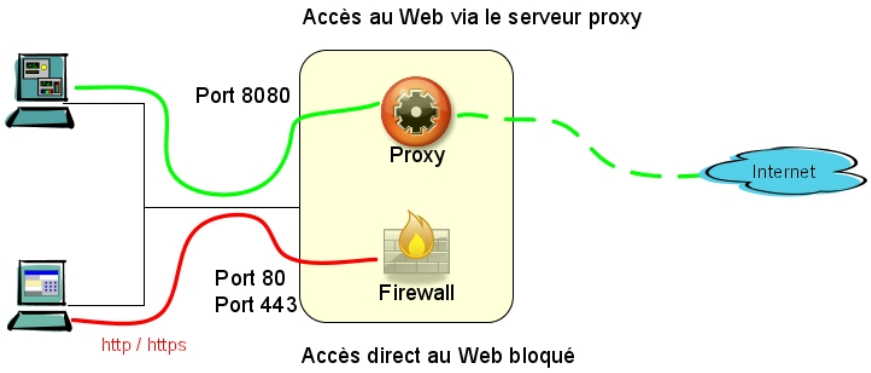


Figure 7.9 : Accès au Web passant uniquement par le serveur proxy

7.3.2 Activation du service proxy cache

Pour activer le service proxy cache :

1. Sélectionnez le menu **Gestion des services > Gestion du service réseau > Service Proxy Cache**.
2. Définissez l'option **Activation du proxy cache** sur la valeur **On**.

7.3.3 Contrôle d'accès au Web

Pour contrôler l'accès au Web :

1. Sélectionnez le menu **Gestion des services > Sécurité > Contrôle d'accès au Web**.
2. Pour chaque utilisateur, indiquez si l'accès au Web est autorisé ou interdit.
3. Sélectionnez **On** pour activer le **Contrôle de la navigation des utilisateurs sur le Web**.

Figure 7.10 : Formulaire de contrôle de l'accès au Web

7.3.4 Filtrage Web

Le service de filtrage Web repose sur des listes d'URL et de mots-clés destinées à interdire/autoriser l'accès au Web :

- Les **black listes** répertorient l'ensemble des URL ou mots-clés dont le contenu associé restera inaccessible par les utilisateurs. Les autres contenus sont accessibles.

  Exemples 1 :
  siteinterdit.com, sexe, .mp3

- Les **white listes** incluent l'ensemble des URL ou mots-clés dont le contenu associé est accessible par les utilisateurs. Les autres contenus ne sont pas accessibles.

  Exemples 2 :
  www.alcatel-lucent.com, .edu

Note :
Le service proxy cache doit être actif pour que le système filtre le trafic Web.

7.3.4.1 Filtrage de l'accès au Web pour tous les utilisateurs

Pour filtrer l'accès au Web pour tous les utilisateurs :

1. Sélectionnez le menu **Gestion des services > Sécurité > Black et White listes**.
2. Sélectionnez l'onglet **Listes principales**.
3. Cliquez sur le bouton situé en regard de la black ou white liste à modifier.
4. Dans l'onglet **Liste** :
   - Saisissez les URL et/ou les mots-clés voulus.
   - Cliquez sur **OK**.

   Note :
   Vous pouvez également modifier les listes à l'aide des options d'exportation et d'importation.
5. Pour que la liste soit automatiquement mise à jour à partir d'un serveur FTP :
   a. Sélectionnez l'onglet **Mise à jour**.
   b. Saisissez les caractéristiques du serveur FTP : nom, chemin, etc.
   c. Cliquez sur **OK**.
6. Revenez au menu **Listes principales**.
7. Activez la liste en cliquant sur **Activé**.

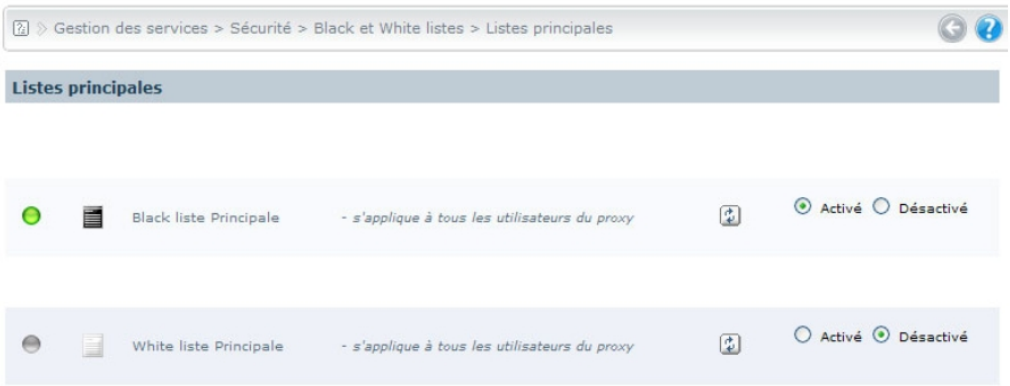

Gestion des services > Sécurité > Black et White listes > Listes principales
Listes principales
Black liste Principale
- s'applique à tous les utilisateurs du proxy
Activé
Désactivé
White liste Principale
- s'applique à tous les utilisateurs du proxy
Activé
Désactivé

Figure 7.11 : Black et white listes pour tous les utilisateurs

7.3.4.2 Filtrage de l'accès au Web pour des groupes d'utilisateurs

Pour filtrer l'accès au Web pour des groupes d'utilisateurs :

1. Sélectionnez le menu **Gestion des services > Sécurité > Black et White listes**.
2. Sélectionnez l'onglet **Listes par groupe**.
3. Dans le formulaire **Listes par groupe** :
   a. Saisissez le nom de la liste.
   b. Précisez le type de liste (black liste ou white liste).
   c. Cliquez sur **AJOUTER**.
   La nouvelle liste apparaît désormais dans le formulaire.

4. Cliquez sur le bouton pour modifier la nouvelle liste.
5. Dans l'onglet **Liste** :
   - Saisissez les URL et/ou les mots-clés voulus.
   - Cliquez sur **OK**.

   Note :
   Vous pouvez également modifier les listes à l'aide des options d'exportation et d'importation.
6. Sélectionnez les groupes souhaités dans l'onglet **Groupes**.
7. Pour que la liste soit automatiquement mise à jour à partir d'un serveur FTP :
   a. Sélectionnez l'onglet **Mise à jour**.
   b. Saisissez les caractéristiques du serveur FTP : nom, chemin, etc.
   c. Cliquez sur **OK**.
8. Revenez au menu **Listes par groupe**.
9. Activez le filtrage **Black et White listes par groupe** en cliquant sur **On**.

Figure 7.12 : Black et white listes pour des groupes d'utilisateurs

7.3.5 Configuration du client

Les postes clients doivent être configurés de manière à pouvoir accéder au serveur proxy.

Pour configurer le navigateur Web d'un poste client :

1. Accédez aux paramètres de connexion du navigateur.
   Par exemple, pour Microsoft Internet Explorer :
   a. Sélectionnez le menu **Outils > Options Internet**.
   b. Sélectionnez l'onglet **Connexions**.
   c. Cliquez sur le bouton **Paramètres réseau**.

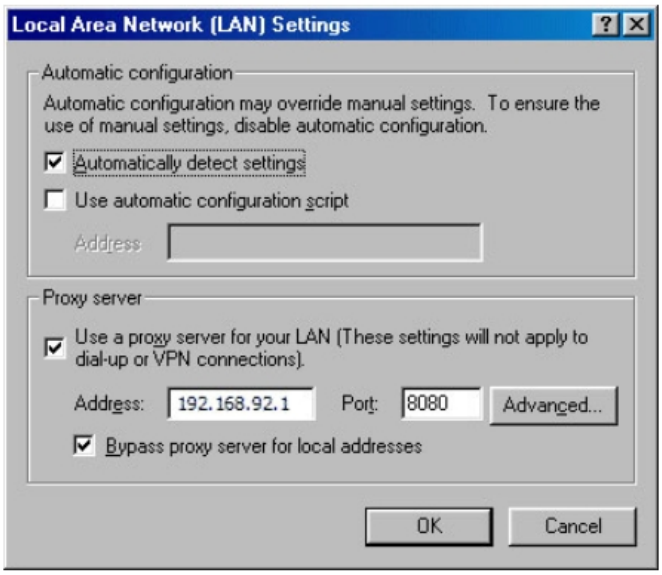

Local Area Network (LAN) Settings
Automatic configuration
Automatic configuration may override manual settings. To ensure the use of manual settings, disable automatic configuration.
Automatically detect settings
Use automatic configuration script
Address
Proxy server
Use a proxy server for your LAN (These settings will not apply to dial-up or VPN connections).
Address: 192.168.92.1
Port: 8080
Advanced...
Bypass proxy server for local addresses
OK
Cancel

Figure 7.13 : Exemple de paramètres (Microsoft Internet Explorer)

Les autres navigateurs Web proposent des paramètres similaires.

2. Saisissez l'adresse du serveur proxy. Par exemple, si le poste appartient au réseau LAN connecté à l'interface LAN1, l'adresse du serveur proxy correspond à l'adresse IP de LAN1.
3. Saisissez le numéro du port proxy : **8080**.

7.3.6 Statistiques du proxy cache

Le proxy cache peut également vous servir à contrôler le trafic Web et générer des rapports.

Pour activer les statistiques du proxy cache :

1. Sélectionnez le menu **Tableau de bord > Analyse des flux du proxy cache**.
2. Cliquez sur **On** pour activer l'option **Activer/désactiver les statistiques**.

7.4 Gestion des certificats

7.4.1 Présentation

Un certificat est un document électronique qui associe une clé à une identité. Il contient une signature numérique délivrée par une autorité de certification.

Parmi d'autres informations, le certificat inclut :

- le nom de l'entreprise,
- la période de validité,
- la signature numérique.

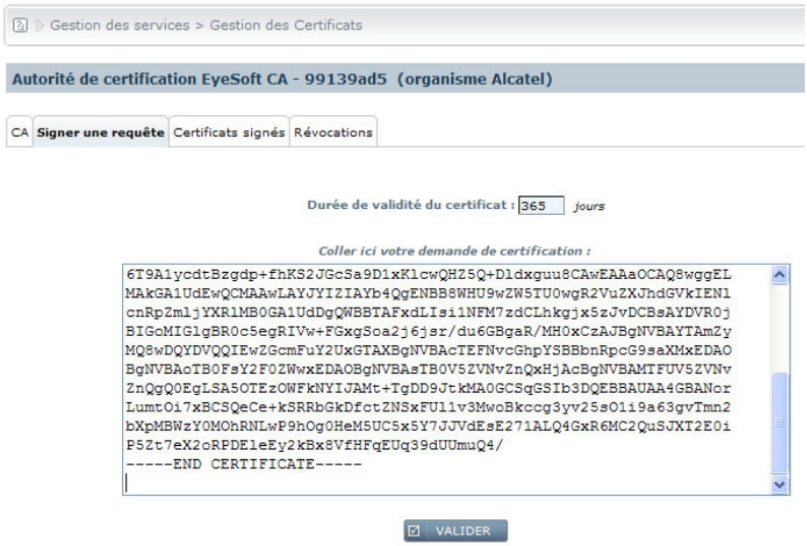
L'Extended Communication Server dispose de sa propre autorité de certification, qui signe les

certificats fournis par le serveur pour tous les services sécurisés.

7.4.2 Création d'un certificat utilisateur

Pour créer un certificat utilisateur :

1. Sélectionnez le menu **Gestion des services > Gestion des certificats**.
2. Sélectionnez l'onglet **Certificats utilisateurs**.
3. Pour créer un certificat privé :
   - **a.** Cliquez sur **Nouveau**.
     Un formulaire s'affiche.
   - **b.** Saisissez les paramètres d'identification de l'entreprise.
   - **c.** Saisissez le nom du certificat.
   - **d.** Cliquez sur **OK**.
     Le certificat est créé, mais n'est pas encore valide, car il n'a pas été signé.
   - **e.** Sélectionnez le certificat et copiez-le vers le Presse-papiers.
4. Sélectionnez l'onglet **Autorités de Certification**.
5. Ouvrez le panneau de l'autorité de certification en cliquant sur .
6. Sélectionnez l'onglet **Signer une requête**.



7. Collez le certificat que vous avez copié.
8. Précisez la période de validité.
9. Cliquez sur **OK**.
   Le certificat est à présent signé et valide.

7.4.3 Utilisation d'un certificat

Une fois le certificat utilisateur créé, vous devez l'affecter aux services. L'exemple ci-dessous indique comment affecter le certificat au service d'accès au Web.

Pour affecter un certificat au service d'accès au Web :

1. Sélectionnez le menu **Gestion du boîtier > Configuration de l'accès depuis une connexion Internet**.
2. Sélectionnez l'onglet **Certificat SSL**.
3. Sélectionnez le certificat de votre choix.

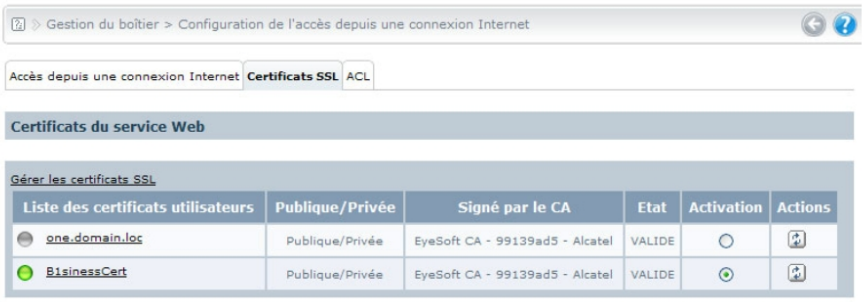


Figure 7.16 : Affectation d'un certificat au service d'accès au Web

Les messages d'alerte de sécurité relatifs aux certificats peuvent concerner :

- la validité de la date (période de validité arrivée à expiration),
- la validité du nom (valeur ne correspondant pas au nom du site),
- l'autorité de certification (autorité inconnue).

Security Alert
Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.
The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certifying authority.
The security certificate date is valid.
The security certificate has a valid name matching the name of the page you are trying to view.
Do you want to proceed?
Yes
No
View Certificate

Figure 7.17 : Exemple d'alerte de sécurité

Afin d'éviter le déclenchement de l'alerte de sécurité illustrée ci-dessus, vous devez obligatoirement installer le certificat sur le périphérique client.

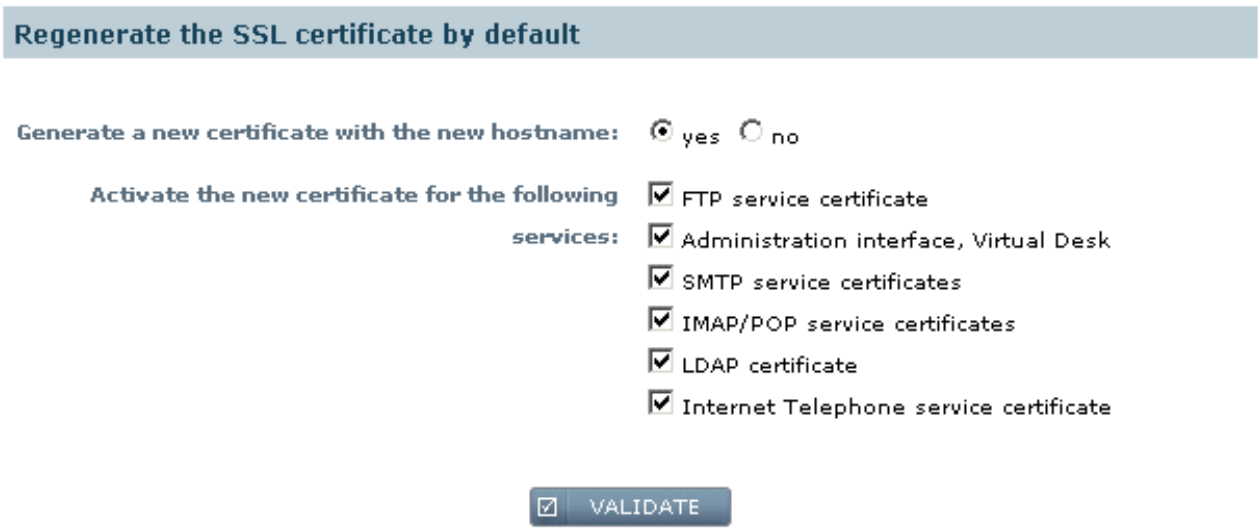
Pour installer le certificat :

1. Sélectionnez le menu **Gestion des services > Gestion des certificats**.
2. Sélectionnez l'onglet **Autorités de Certification**.
3. Ouvrez le panneau de l'autorité de certification en cliquant sur .
4. Cliquez sur **Cliquez ici pour exporter le certificat**.
5. Une boîte de dialogue s'affiche et vous propose diverses options :
   - Cliquez sur **Ouvrir** pour installer le certificat sur la machine actuelle. Vous devez alors répéter la procédure sur chaque machine.
   - Cliquez sur **Enregistrer** pour installer ultérieurement le certificat sur toutes les machines, à partir du fichier que vous enregistrez.

7.4.4 Activation de la regénération automatique des certificats

Les certificats dépendent du nom d'hôte attribué à l'Extended Communication Server. Par conséquent, leur regénération est nécessaire après chaque modification du nom d'hôte. Il est toutefois possible d'activer une option permettant de regénérer automatiquement les certificats en cas de modification du nom d'hôte de l'Extended Communication Server.

1. Sélectionnez le menu **Gestion des services** > **Gestion du service réseau** > **Paramètres Réseau Généraux**.
   Si vous avez déjà généré et signé des certificats, la fenêtre présente un formulaire intitulé **Regénérer le certificat SSL par défaut**.



2. Indiquez si vous souhaitez regénérer automatiquement les certificats en cas de modification du nom d'hôte. Cliquez sur **Oui** ou **Non**.

3. Sélectionnez les services auxquels les nouveaux certificats doivent être affectés.

Chapitre

8

Convergence voix/données

Lisez ce chapitre si votre Extended Communication Server fonctionne de pair avec un OmniPCX Office. À l'issue de ce chapitre, vous saurez effectuer la convergence des services Internet et de téléphonie.

8.1 Généralités

Le service de convergence voix/données permet aux utilisateurs d'accéder aux fonctions de téléphonie depuis le Bureau Virtuel et de bénéficier de services supplémentaires sur les postes téléphoniques : renvoi des appels, messagerie unifiée, fonction click to call, etc.

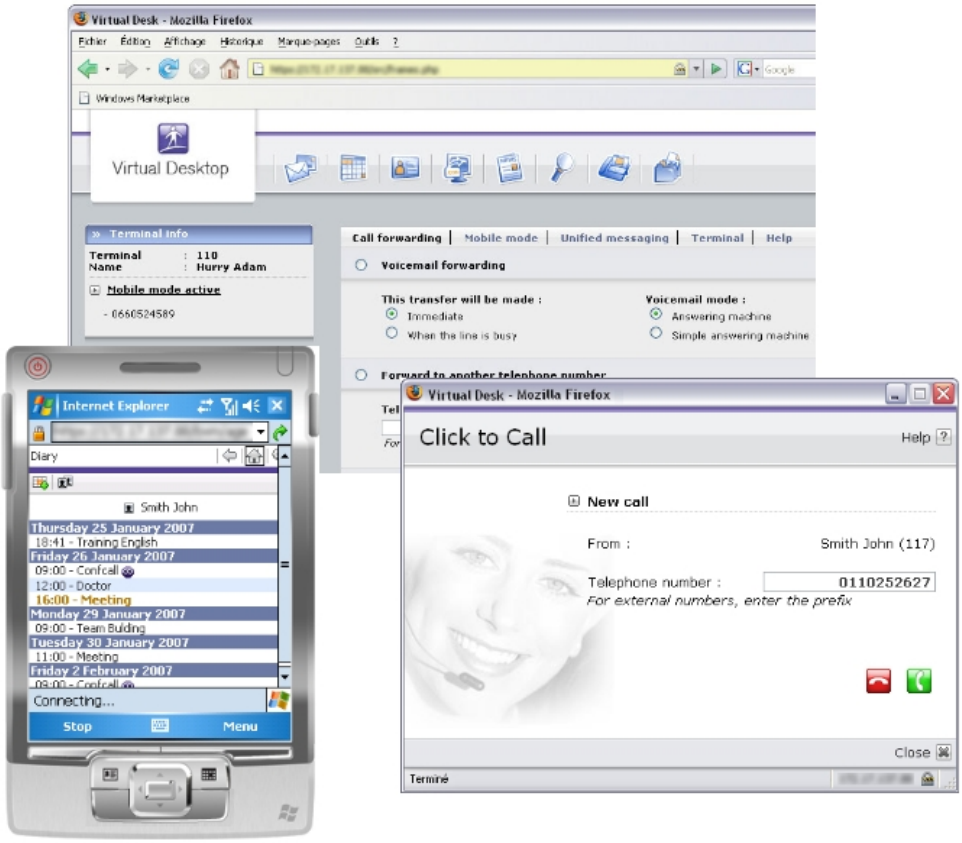


Figure 8.1 : Convergence voix/données

Le pack Extended Communication doit être installé pour pouvoir accéder au menu **OmniPCX Office** dans le panneau **Gestion des services**.

Figure 8.2 : Icône et menu OmniPCX Office

8.2 Activation de la convergence voix/données

Note :
Dans une optique d'efficacité, nous vous recommandons d'installer l'Extended Communication Server et l'OmniPCX Office sur le même sous-réseau.

Pour activer la convergence voix/données :

1. Sélectionnez le menu **Gestion des services > OmniPCX Office > Détection et Configuration**.
2. Sélectionnez l'onglet **Détection IP**.
3. Cliquez sur **DÉTECTION DE L'IP DE L'OMNIPCX OFFICE**.
   Après quelques secondes, l'adresse IP de l'OmniPCX Office s'affiche à l'écran.
4. Si la détection automatique échoue :
   a. Dans le champ **Adresse IP OmniPCX Office**, saisissez l'adresse IP de l'OmniPCX Office.
   b. Cliquez sur **VALIDER**.
5. Définissez l'option **Etat du Service de Convergence Voix / Données** sur **On**.

Figure 8.3 : Activation du service de convergence voix/données

8.3 Récupération des informations

Une fois le service activé, vous pouvez récupérer des informations depuis l'OmniPCX Office:

- Utilisez le menu **Synchronisation et Gestion des postes** pour récupérer la liste des postes ou périphériques téléphoniques connectés à l'OmniPCX Office. Cette fonction vous permet de synchroniser les comptes utilisateurs avec les tableaux des postes téléphoniques.
- Utilisez le menu **Import utilisateurs** pour créer des comptes utilisateurs à partir du tableau des utilisateurs de l'OmniPCX Office. Cette opération permet de créer automatiquement des comptes utilisateurs à partir des informations récupérées de l'OmniPCX Office (nom, prénom, numéros internes). Vous pouvez modifier ces comptes ultérieurement afin d'ajouter des informations requises par l'Extended Communication Server.
- Chaque poste synchronisé doit à présent être associé avec un compte utilisateur existant ou nouvellement créé.

Reportez-vous à l'aide en ligne pour plus de détails.

Chapitre 8 *Convergence voix/données*

Chapitre 9

Gestion de la messagerie

À l'issue de ce chapitre, vous saurez comment gérer la messagerie interne et externe.

9.1 Généralités

L'Extended Communication Server inclut un serveur de messagerie, qui peut être utilisé comme serveur autonome ou bien être relayé par un serveur de messagerie externe.

Le service de messagerie de l'Extended Communication Server prend en charge les protocoles suivants :

- SMTP (Simple Mail Transfer Protocol), pour la réception des e-mails
- POP (Post Office Protocol) ou IMAP (Internet Message Access Protocol) pour l'envoi des e-mails

Pour que le service de messagerie puisse fonctionner correctement, il est nécessaire d'activer le protocole SMTP. Si vous utilisez un client lourd de messagerie, activez également le service POP ou IMAP.

Dans la mesure où différentes configurations permettent de rendre le service de messagerie disponible, les sections suivantes vous présentent le paramétrage de ce service en quatre étapes :

1. Messagerie interne, permettant aux utilisateurs d'échanger des e-mails au sein de l'entreprise
2. Messagerie externe, permettant aux utilisateurs d'envoyer et de recevoir des messages via Internet
3. Configuration pour un client lourd de messagerie
4. Paramètres supplémentaires pouvant être utiles, en fonction des caractéristiques de l'entreprise. Pour plus d'informations, vous pouvez aussi consulter l'aide en ligne.

Note :

Nous vous recommandons de tester le service de messagerie à partir de sessions du Bureau Virtuel.

9.2 Messagerie interne

Pour activer le service de messagerie interne :

1. Sélectionnez le menu **Gestion des services > Messagerie > SMTP**.
2. Définissez l'option **Statut SMTP** sur la valeur **On**.

Tous les utilisateurs disposant d'une adresse e-mail et des autorisations nécessaires peuvent à présent échanger des e-mails en interne.

9.3 Extension du service à Internet

Le service SMTP doit être configuré pour pouvoir étendre le service de messagerie à Internet.

Pour configurer le service SMTP pour Internet :

1. Sélectionnez le menu **Gestion des services > Messagerie > SMTP > Configuration de base**.

2. Sélectionnez l'onglet **Mode d'envoi**.
3. Saisissez l'adresse e-mail qui recevra les messages en erreur.
4. Si l'enterprise possède un **nom de domaine public**, sélectionnez **Utiliser le mode Internet**.
   Les e-mails sont alors échangés directement avec les autres serveurs de messagerie via Internet.

   Note 1 :
   Assurez-vous que l'enregistrement DNS MX (Mail eXchange) pointe vers l'adresse IP publique du serveur. Contactez le bureau d'enregistrement qui gère le nom du domaine afin de vérifier ce paramètre.

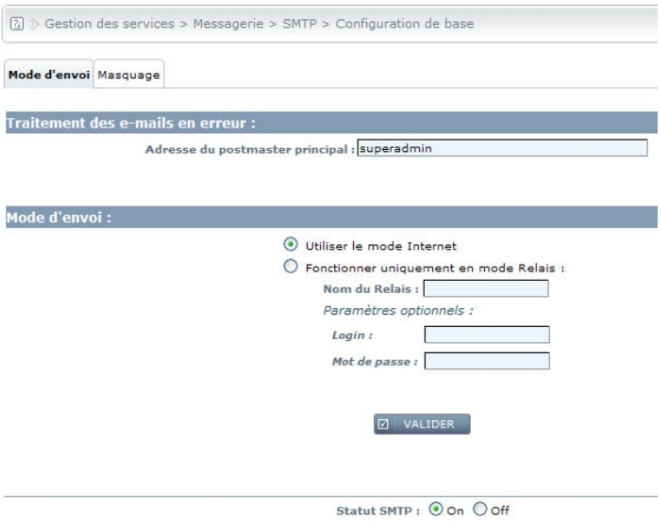


Figure 9.1 : Accès direct aux serveurs de messagerie

5. Si l'entreprise ne possède pas de nom de domaine public :
   a. Sélectionnez **Fonctionner uniquement en mode Relais**.
   Les e-mails sont alors échangés avec le serveur de messagerie du FAI (Fournisseur d'accès Internet). Le serveur joue le rôle de relais du serveur de messagerie de l'Extended Communication Server.

   Note 2 :
   Le nom du relais, le login et le mot de passe sont fournis par le FAI.
   b. Saisissez le nom du relais ou son adresse IP.
   c. Saisissez les login et mot de passe, si le serveur de messagerie du FAI les réclame.

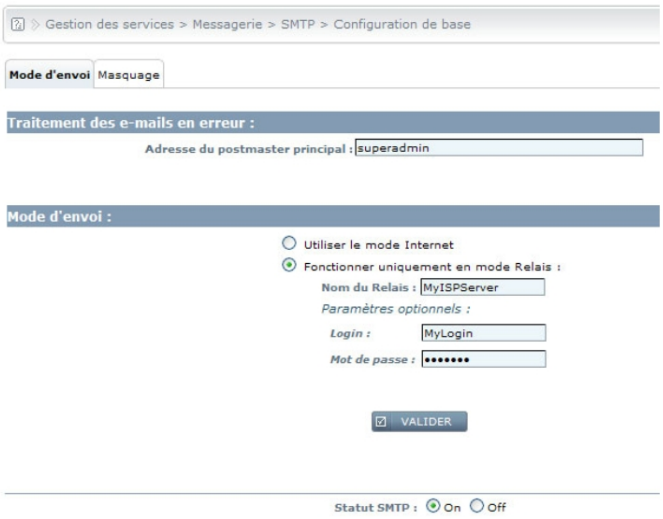

Gestion des services > Messagerie > SMTP > Configuration de base
Mode d'envoi
Masquage
Traitement des e-mails en erreur :
Adresse du postmaster principal : superadmin
Mode d'envoi :
Utiliser le mode Internet
Fonctionner uniquement en mode Relais :
Nom du Relais : MyISPServer
Paramètres optionnels :
Login : MyLogin
Mot de passe : •••••••
VALIDER
Statut SMTP : On Off

Figure 9.2 : Fonctionnement en mode relais

d. Cliquez sur **VALIDER**.

9.4 Configuration pour un client lourd de messagerie

D'autres paramétrages sont nécessaires lorsque vous utilisez un client lourd de messagerie tel que Microsoft Outlook ou Mozilla Thunderbird.

Côté serveur, vous devez activer le service POP ou IMAP :

1. Sélectionnez le menu **Gestion des services > Messagerie > POP/IMAP**.
2. Affectez la valeur **On** à l'option **POP Statut** ou **IMAP Statut**, ou aux deux.

Côté client, vous devez configurer chaque compte de messagerie en fonction des paramètres du serveur :

- Protocole
- Identifiant et mot de passe de l'utilisateur

9.5 Paramètres supplémentaires

9.5.1 Noms de domaine

Utilisez le menu **Noms de domaines** si plusieurs noms de domaine doivent être utilisés.

Par défaut, le système ne prend en charge qu'un seul nom de domaine, qui correspond au nom de domaine principal que vous avez déclaré dans le formulaire **Paramètres Réseau Généraux**. Si l'entreprise possède plusieurs noms de domaine, définissez-les tous dans le système afin d'optimiser le traitement des e-mails. Aucune requête DNS externe n'est requise lorsque les adresses e-mail appartiennent aux domaines déclarés dans le système.

Pour déclarer un nom de domaine dans le système :

1. Sélectionnez le menu **Gestion des services > Messagerie > SMTP > Noms de**

domaines.

2. Cliquez sur **Ajouter**.
   Le formulaire **Déclaration des noms de domaines gérés par l'Appliance** s'affiche.

Gestion des services > Messagerie > SMTP > Noms de domaines
Déclaration des noms de domaines gérés par l'Appliance
Nom de domaine : bus1ness.net
Transport : Local
Via SMTP
Nom du serveur : MailServ2
Paramètres optionnels :
Login :
Mot de passe :
VALIDER

Figure 9.3 : Formulaire de déclaration des noms de domaine

3. Saisissez le nouveau nom de domaine.
4. Sous **Transport** :
   - Sélectionnez l'option **Local** si le serveur de messagerie gère tous les e-mails appartenant à ce domaine.
   - Sélectionnez l'option **Via SMTP** si plusieurs serveurs de messagerie gèrent les e-mails appartenant à ce domaine.
     Dans ce cas, le serveur de messagerie tente d'abord de traiter l'e-mail à partir de ses propres tables. Si l'adresse e-mail ne figure pas dans ces tables, le message est envoyé au serveur de messagerie suivant via le protocole SMTP. Identifiez ce nouveau serveur en renseignant le champ **Nom du serveur**. Vous pouvez également saisir son **Login** et son **Mot de passe**, si nécessaire.
     Plusieurs serveurs de messagerie peuvent être reliés de cette manière.
5. Cliquez sur **VALIDER**.

Une fois le nouveau nom de domaine déclaré, vous pouvez créer des adresses e-mails pour chaque utilisateur nécessitant une adresse associée à ce nom de domaine.

L'exemple ci-dessous illustre la liste des noms de domaine suite à la création d'un deuxième nom de domaine.

Gestion des services > Messagerie > SMTP > Noms de domaines
Déclaration des noms de domaines gérés par l'Appliance
Nom de domaine :
b1server.bus1ness.com
bus1ness.com Local
bus1ness.net Vers le serveur : MailServ2
AJOUTER

Figure 9.4 : Liste des noms de domaine

9.5.2 Anti-relais / Autorisation de relais

Cette fonction a pour but de préserver le serveur de messagerie de toute utilisation malveillante, comme le relais de spams. Utilisez-la afin de contrôler les droits d'accès aux services de messagerie accordés aux utilisateurs, notamment aux utilisateurs distants. Par défaut, les utilisateurs se trouvant derrière l'interface LAN1 sont autorisés à utiliser le serveur de messagerie de l'Extended Communication Server comme relais vers Internet.

Pour gérer la fonction de relais/anti-relais :

1. Sélectionnez le menu **Gestion des services > Messagerie > SMTP > Anti-relais / Autorisation de relais**.
   Un panneau à onglets s'affiche avec la liste des interfaces réseau et des autorisations de relais.

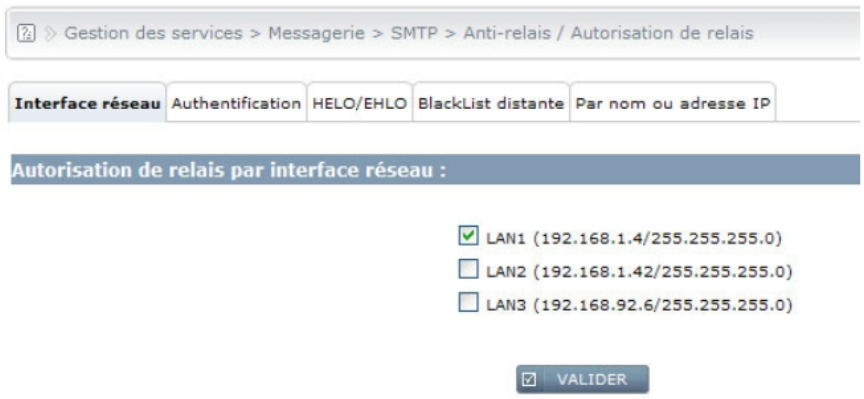


Figure 9.5 : Panneau à onglets Autorisation de relais

2. Sélectionnez les interfaces réseau souhaitées.
   Lorsque vous sélectionnez une interface réseau, seuls les utilisateurs locaux situés derrière cette dernière peuvent accéder à Internet.
   Pour les utilisateurs distants, vous devez configurer les autorisations décrites aux étapes suivantes.
3. Pour autoriser le relais vers Internet via l'authentification du client :
   - Sélectionnez l'onglet **Authentification**.
   - Définissez l'option **Autoriser le relais** sur **Oui**.
   - Cliquez sur **VALIDER**.

     Note :
     Le client de messagerie des utilisateurs distants doit être configuré pour exiger une authentification lors de l'accès au service.
4. Pour autoriser le relais vers Internet par un nom ou une adresse IP :
   - Sélectionnez l'onglet **Par nom ou adresse IP**.
   - Cliquez sur **Ajouter**.
   - Saisissez le nom souhaité ou l'adresse IP.

- Cliquez sur VALIDER.

Les autres onglets (**HELO/EHLO** et **BlackList distante**) peuvent également être utilisés pour restreindre les autorisations et filtrer les adresses e-mail.

9.5.3 Messagerie distante

Utilisez ce menu pour récupérer des e-mails provenant de comptes mutuels ou pour autoriser les utilisateurs à récupérer leur propre compte de messagerie.

Pour activer la messagerie distante :

1. Sélectionnez le menu **Gestion des services > Messagerie > Messagerie distante**.
2. Sélectionnez l'onglet **Fréquence**.
3. Si vous voulez modifier la fréquence à laquelle les e-mails sont récupérés :
   - Saisissez la fréquence de récupération des e-mails. Par défaut, elle est fixée à 15 minutes.
   - Cliquez sur **VALIDER**.
4. Définissez l'option **Statut du rapatriement** sur **On**.
   Ces premières étapes suffisent pour permettre aux utilisateurs de gérer leur propre compte de messagerie via le Bureau Virtuel.
   Vous pouvez également exécuter les étapes suivantes si les e-mails sont récupérés à partir de comptes mutuels (une boîte de réception par domaine) hébergés par le FAI, ou bien si les e-mails sont stockés par le FAI et récupérés à la demande via une commande ETRN (lorsque la connexion à Internet est temporaire, par exemple).
5. Lorsque vous devez gérer des comptes mutuels :
   a. Sélectionnez l'onglet **Comptes mutuels**.
   b. Sélectionnez le protocole et saisissez les informations nécessaires relatives au serveur de messagerie du FAI.
   c. Configurez le service de récupération.
   d. Cliquez sur **VALIDER**.
6. Si le serveur distant est un serveur ETRN (Extended Turn) :
   a. Sélectionnez l'onglet **ETRN**.
   b. Saisissez le nom du serveur.
   c. Définissez l'option **Activer la récupération** sur **Oui**.
   d. Cliquez sur **VALIDER**.

9.5.4 Filtrage des mails

Cette fonction repose sur plusieurs services de filtrage que vous pouvez activer et configurer séparément. Vous pouvez filtrer les messages en fonction de l'adresse e-mail, de leur contenu ou des pièces jointes qu'ils contiennent.

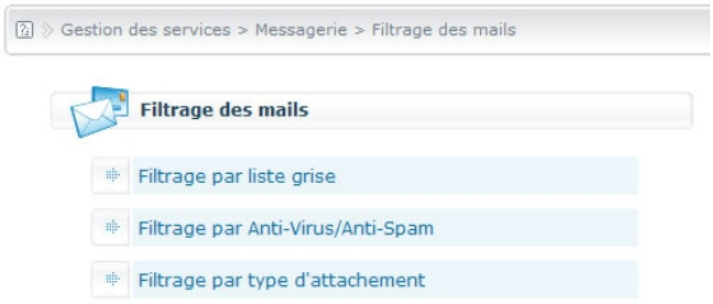

Gestion des services > Messagerie > Filtrage des mails
Filtrage des mails
Filtrage par liste grise
Filtrage par Anti-Virus/Anti-Spam
Filtrage par type d'attachement

Figure 9.6 : Services Filtrage des mails

Le menu **Gestion des services > Messagerie > Filtrage des mails** est divisé en trois sous-menus correspondant à trois services complémentaires :

- Le **Filtrage par liste grise** utilise la méthode de liste grise pour filtrer les e-mails entrants. L'agent de transfert de messagerie rejette temporairement tout e-mail envoyé par un expéditeur inconnu. Si l'e-mail est légitime, le serveur d'origine essaiera de le renvoyer ultérieurement et l'agent l'acceptera à ce moment. En revanche, si l'e-mail provient d'un spammer, il ne sera probablement pas renvoyé.

  Afin d'éviter que des e-mails importants ne soient retardés ou rejetés, l'administrateur conserve une white liste dans laquelle sont répertoriées toutes les adresses autorisées. Il peut également permettre aux utilisateurs de gérer leur propre white liste.

- Le service **Filtrage par Anti-Virus/Anti-Spam** repose sur trois plugins :
  - ClamAV (Clam AntiVirus) est un utilitaire anti-virus libre utilisé principalement pour analyser les virus contenus dans les e-mails. Il est pré-installé et libre de droit. En revanche, il n'analyse pas les flux http et ftp du trafic.
  - SpamAssassin est un programme de filtrage des spams. Il est pré-installé et libre de droit.
  - Kasperky est un utilitaire anti-virus puissant, qui nécessite une licence.

  Activez le service via le menu **Configuration des plugins** et configurez chaque plugin séparément.

- Le service **Filtrage par type d'attachement** filtre les e-mails selon le type d'extension ou le type de MIME (Multipurpose Internet Mail Extensions) des fichiers joints aux e-mails.

Chapitre 9 *Gestion de la messagerie*

Chapitre

10

Hébergement Web

À l'issue de ce chapitre, vous aurez un aperçu du service d'hébergement Web de l'Extended Communication Server et saurez comment créer un site Web hébergé sur ce serveur.

10.1 Présentation de l'hébergement de sites

L'Extended Communication Server peut être utilisé afin d'héberger un ou plusieurs sites Web comme :

- Un site Intranet, permettant de partager et de diffuser les informations en interne. Ce type de site est associé à une interface réseau privée (LAN).
- Un site Extranet, permettant à des utilisateurs externes (clients, fournisseurs ou partenaires autorisés) d'accéder à une partie des informations internes. Ce type de site est associé à une interface réseau publique (WAN) et son contenu est protégé par un système d'authentification.
- Un site Internet, pour diffuser plus largement les informations et accroître la visibilité de l'entreprise. Ce type de site est associé à une interface réseau publique (WAN) et accessible sans authentification.

Grâce à cette solution, l'entreprise reste propriétaire de ses propres données au lieu de les confier à un tiers, ce qui réduit considérablement les coûts et les risques de piratage.

Note :

L'hébergement d'un site Internet ou Extranet nécessite une bande passante suffisamment large capable de prendre en charge le nombre de connexions attendues sur le site en question.

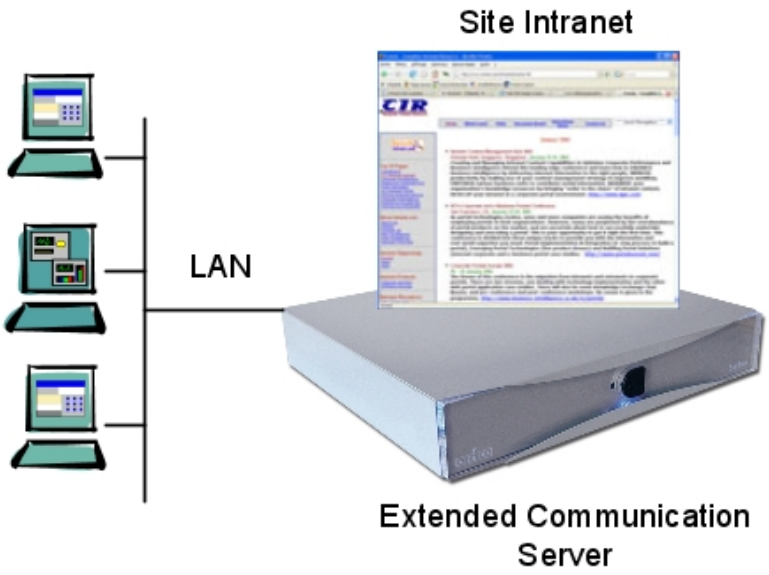


Figure 10.1 : Site Intranet hébergé en local

Pour créer un site hébergé en local, vous devez exécuter les procédures décrites dans les sections suivantes, en respectant l'ordre indiqué.

10.2 Configuration du service d'hébergement

10.2.1 Indication du webmaster

Le webmaster du site peut être :

- l'administrateur du serveur, identifié par le login **superadmin** (par défaut, l'administrateur est le webmaster),
- un administrateur délégué, cet utilisateur possédant certains droits, notamment la gestion du site.

L'administrateur du serveur peut octroyer les droits d'administrateur délégué à un utilisateur lors de la création ou la modification des comptes utilisateurs (menu **Annuaire > Comptes utilisateurs**).

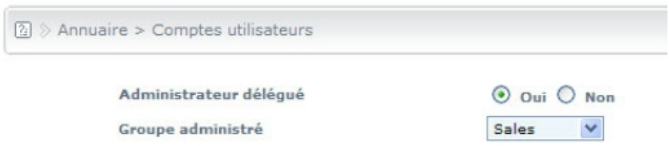


Figure 10.2 : Affectation des droits d'administrateur délégué à un utilisateur

Si c'est un administrateur délégué qui occupera la fonction de webmaster, l'administrateur du serveur doit d'abord définir les droits de ce dernier.

Pour déclarer un administrateur délégué comme webmaster :

1. Depuis l'interface d'administration, sélectionnez le menu **Gestion des services> Web > Administration déléguée**.
2. Cliquez sur **Ajouter**.
3. S'il existe plusieurs administrateurs délégués, sélectionnez celui approprié.
4. Cliquez sur **Ajouter**.
   Un panneau à onglets s'affiche.

Gestion des services > Web > Administration déléguée
Param.Généraux
Ajout d'une IP
Liste des IP utilisées
Politique d'attribution des adresses IP : Résolution DNS par nom
- Nombre de sites autorisés : 0
Pour modifier la politique d'attribution des adresses IP d'un utilisateur, ce dernier ne doit utiliser aucune adresse IP.
Autoriser la configuration des CGI : oui
non
VALIDER

Figure 10.3 : Panneau à onglets pour les droits du webmaster

5. Définissez les droits du webmaster :
   a. Dans l'onglet **Param. Généraux**, indiquez le nombre de sites autorisés et renseignez les autres champs.
   b. Cliquez sur **VALIDER**.
   c. Dans l'onglet **Ajout d'une IP**, indiquez quelle adresse IP (interface réseau) vous souhaitez affecter à ce webmaster.
   d. Cliquez sur **VALIDER**.
   L'onglet **Liste des IP utilisées** contient à présent les adresses IP que vous avez affectées.

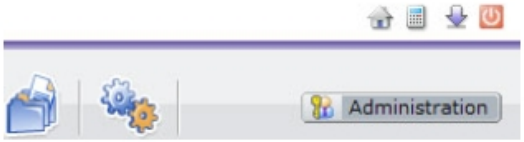
Figure 10.4 : Adresses IP affectées au webmaster

10.2.2 Création du site

Important :
Le site doit être créé à partir du compte du webmaster. La procédure suivante s'adresse donc au webmaster.

Pour créer le site :

1. Accédez à l'interface d'administration :
   - Si vous êtes webmaster et administrateur du serveur, l'interface d'administration est déjà ouverte.
   - Si vous êtes webmaster et administrateur délégué, cliquez sur le bouton **Administration** situé sur le côté droit de votre Bureau Virtuel.
     L'interface d'administration s'ouvre et propose uniquement les menus et ressources que vous êtes autorisé à utiliser/gérer.



2. Sélectionnez le menu **Gestion des services > Web > Configuration des sites Web**.
   Un panneau à onglets s'affiche.
3. Sélectionnez l'onglet correspondant au type de site concerné.
   - **Sites Web : par nom** (http)
   - **Sites Web : par IP** (http)
   - **Sites Web sécurisés : par IP** (https)
4. Cliquez sur **Ajouter**.
5. En fonction du type sélectionné, saisissez le nom complet du site (www.bus1ness.com, par exemple) ou l'adresse IP.
6. Sélectionnez l'interface réseau utilisée pour accéder au site Web :
   - Interface WAN pour un site Internet ou Extranet
   - Interface LAN pour un site Intranet
7. Cliquez sur **VALIDER**.
   Le nouveau site Web apparaît désormais dans la liste des serveurs Web.
8. Pour activer le site, cliquez sur le bouton **Statut**. Le bouton orange devient vert.

Gestion des services > Web > Configuration des sites Web
Sites Web : par nom
Sites Web : par IP
Sites Web sécurisés : par IP
Liste des serveurs Web résolus par leur nom
Nom du serveur
Adresse IP
Statut
Stats
www.bus1ness.com
192.168.1.42 (WAN)

Figure 10.6 : Liste de sites Web

10.2.3 Association d'une base de données au site

Au besoin, une ou plusieurs bases de données peuvent être associées au site Web.

L'Extended Communication Server prend en charge deux systèmes de gestion de bases de données :

- PostgreSQL
- MySQL

Important :

- ***L'administrateur du serveur crée la base de données et l'associe au site précédemment créé par le webmaster.***
- ***La base de données porte le même nom que le site Web associé.***
- ***Le webmaster gère la base de données.***

Par exemple, pour créer une base de données MySQL :

1. Sélectionnez le menu **Gestion des services > Bases de données > MySQL**.

2. Dans la liste **Sélectionner un nom de domaine**, choisissez le site Web concerné.
3. Cliquez sur **Ajouter**.
   Le nom de la base de données et le nom de son administrateur apparaissent dans le formulaire.
4. Cliquez sur **VALIDER**.
   Un message s'affiche dans le formulaire pour confirmer la création de la base de données.

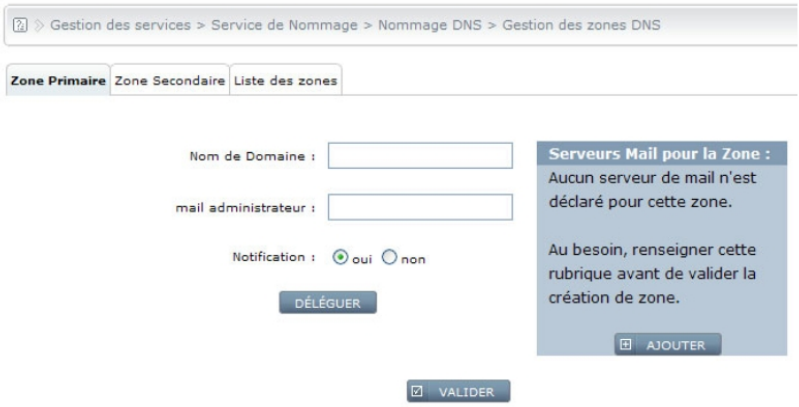
10.2.4 Résolution de noms

Pour un site Internet ou Extranet, la résolution de noms repose sur le nom du domaine public.

Pour un site Intranet, la résolution de noms doit être configurée en local.

Pour configurer la résolution de noms :

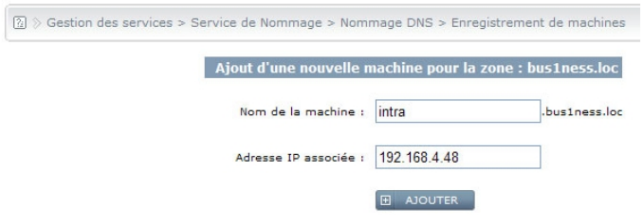
1. Sélectionnez le menu **Gestion des services > Service de Nommage > Nommage DNS > Gestion des zones DNS**.


Gestion des services > Service de Nommage > Nommage DNS > Gestion des zones DNS
Zone Primaire
Zone Secondaire
Liste des zones
Nom de Domaine :
mail administrateur :
Notification : oui non
DÉLÉGUER
Serveurs Mail pour la Zone :
Aucun serveur de mail n'est déclaré pour cette zone.
Au besoin, renseigner cette rubrique avant de valider la création de zone.
AJOUTER
VALIDER

2. Sélectionnez l'onglet **Zone Primaire**.
3. Entrez le nom de domaine (nom du site Intranet).

   Exemples 1 :
   Dans l'URL intra.bus1ness.loc, le nom du domaine est bus1ness.loc.
   Dans l'URL www.bus1ness.com, le nom du domaine est bus1ness.com.
4. Saisissez l'adresse e-mail de l'administrateur.
5. Cliquez sur **VALIDER**.
6. Sélectionnez le menu **Gestion des services > Service de Nommage > Nommage DNS > Enregistrement de machines**.
7. Cliquez sur le bouton **Modifier** qui correspond au site.
8. Dans la partie **Machines enregistrées** du formulaire, cliquez sur **Ajouter**.
9. Saisissez le nom de la machine.

   Exemples 2 :
   Dans l'URL intra.bus1ness.loc, le nom de la machine est intra.
   Dans l'URL www.bus1ness.com, le nom de la machine est www.
10. Saisissez l'adresse IP associée.
11. Cliquez sur **AJOUTER**.
12. Cliquez sur **VALIDER**.


Gestion des services > Service de Nommage > Nommage DNS > Enregistrement de machines
Ajout d'une nouvelle machine pour la zone : bus1ness.loc
Nom de la machine :
intra
.bus1ness.loc
Adresse IP associée :
192.168.4.48
AJOUTER

13. Définissez le champ **Etat du serveur DNS** sur **Actif**.

10.3 Chargement du site sur le serveur

Deux méthodes vous sont proposées pour charger le site sur le serveur :

- FTP (seulement pour le webmaster)
- Voisinage réseau Microsoft

10.3.1 Chargement via FTP

Le webmaster peut utiliser n'importe quel utilitaire FTP.

Les paramètres suivants doivent être renseignés :

- Adresse IP. Cette adresse ne dépend pas de l'interface réseau utilisée pour accéder au site. Elle est liée à la configuration FTP (voir menu **Gestion des services > Gestion du service FTP > Serveur FTP standard**).
- Identifiant et mot de passe du webmaster
- Destination (répertoire **/groupesftp/<nom_site_Web>/html**)

10.3.2 Chargement via le voisinage réseau Microsoft

Le webmaster dispose de plusieurs manières pour accéder au site Web, comme par exemple l'adresse **\\<nom_NetBIOS_ECS>\<nom_site_web>**. Le nom NetBIOS est disponible dans l'onglet **Configuration** du menu **Gestion des services > Serveur de fichiers et contrôleur de domaine > Configuration générale**.

Le webmaster copie ensuite les données du site Web dans le répertoire **html**.

10.4 Limites et restrictions

L'Extended Communication Server prend en charge les protocoles et outils suivants :

- Apache-Tomcat : version 5.5.12
- php : version 5.1.4
- MySQL : version 4.1.19
- PostgreSQL : version 8.0.7

Chapitre 11

Mobilité

11.1 Push Mobile

À l'issue de cette section, vous serez à même de mettre en œuvre le service Push Mobile.

11.1.1 Présentation

Le service Push Mobile permet :

- La synchronisation d'e-mails de l' Extended Communication Server vers un périphérique exécutant Windows Mobile 5 ou 6. Pour cela, le service Push Mobile vérifie régulièrement (par défaut toutes les cinq minutes) la présence de nouveaux e-mails sur les comptes utilisateur de l'Extended Communication Server. Si tel est le cas, les e-mails reçus depuis la dernière synchronisation (ou au cours des cinq derniers jours pour une première synchronisation) sont transférés vers le périphérique mobile.
- La synchronisation des éléments groupware (contacts, événements et tâches de calendrier), entre l'Extended Communication Server et un périphérique exécutant Windows Mobile 5 ou 6. Pour cela, le service Push Mobile vérifie régulièrement (par défaut toutes les cinq minutes) la présence de nouveaux éléments groupware sur les comptes utilisateur de l'Extended Communication Server. Le cas échéant, les éléments groupware créés depuis la dernière synchronisation dans le compte utilisateur de l'Extended Communication Server concerné sont transférés vers le périphérique mobile. Inversement, les éléments groupware créés à l'aide du périphérique mobile sont également transférés vers le compte utilisateur de l'Extended Communication Server.

  Note :
  Si le compte utilisateur de l'Extended Communication Server ne contient aucun élément groupware nouveau, la synchronisation automatique du périphérique vers le compte utilisateur n'est pas effectuée. Vous devez alors déclencher la synchronisation manuellement.

11.1.2 Pré-requis

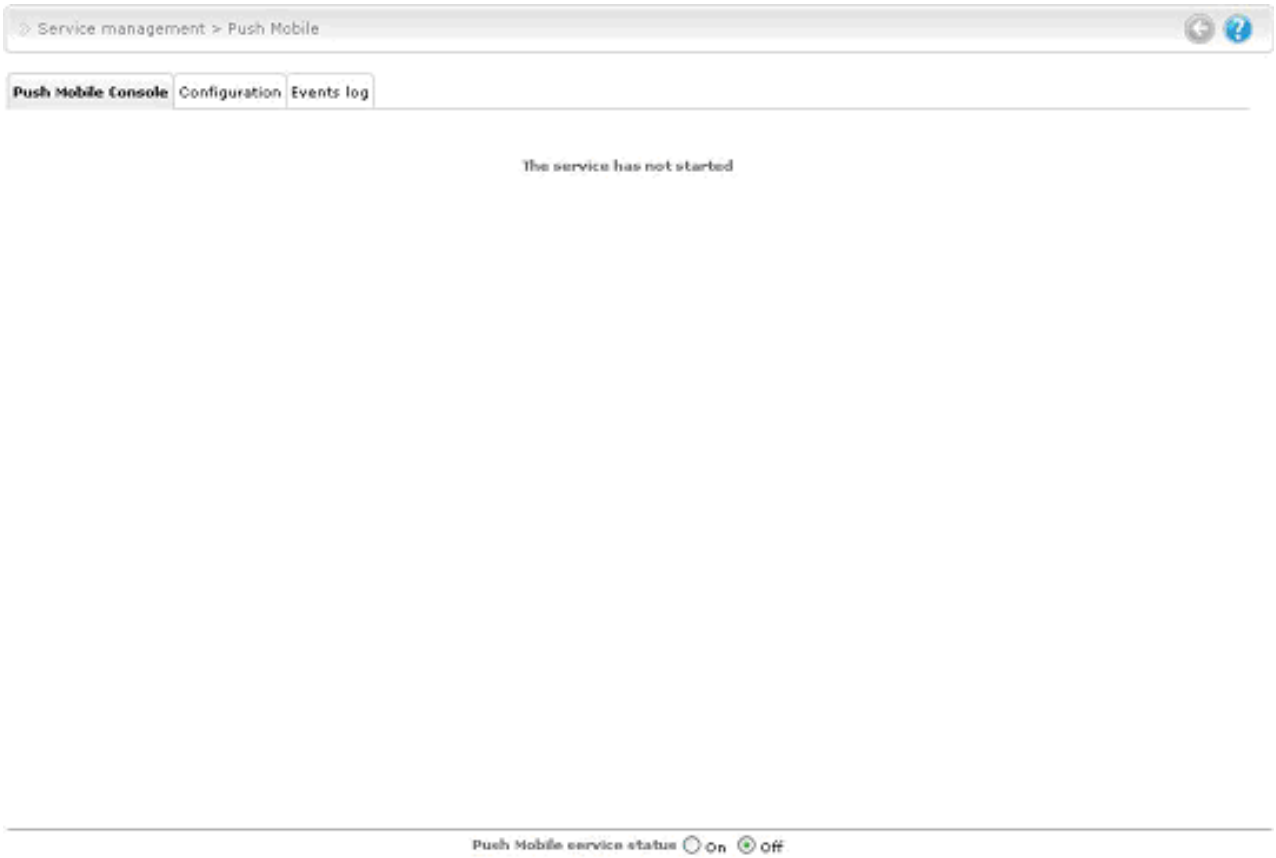
Avant d'activer et de configurer le service Push Mobile, vous devez .

- Installer le service pack correspondant.
- Saisir le numéro de licence.

11.1.3 Activation du service Push Mobile

Pour activer le service Push Mobile :

1. Sélectionnez le menu **Gestion des services** > **Push Mobile**.



2. Activez le service Push Mobile en cliquant sur l'état **On**.
   Une connexion au serveur de relais Push Mobile sur le port https (443) est établie afin d'extraire les informations suivantes :
   - ComID : Identifiant Extended Communication Server sur le serveur de relais Push Mobile. ComID est un identifiant unique fourni par le serveur de relais à l'Extended Communication Server qui fait appel au service Push Mobile.
   - Nombre total d'utilisateurs autorisés. Ce chiffre doit correspondre à votre licence.
   - Nombre de licences utilisées. Il s'agit du nombre d'utilisateurs faisant actuellement appel au service Push Mobile. Ce chiffre est égal à 0 à la première activation du service.
   - Liste des utilisateurs autorisés. Cette liste est vide à la première activation du service.

   Après quelques minutes, l'état de la connexion passe au vert.

11.1.4 Configuration du service Push Mobile

Vous pouvez configurer la fréquence de synchronisation des e-mails et des événements groupware.

Note :
La fréquence de synchronisation ne doit pas être fixée à moins d'une minute pour éviter les encombrements du réseau.

11.1.5 Configuration des accès utilisateur au service Push Mobile

Pour accorder ou refuser à un utilisateur le droit d'accéder au service Push Mobile :

1. Sélectionnez le menu **Répertoire** > **Comptes utilisateur**.
2. Pour chaque utilisateur, autorisez ou interdisez l'**Accès au Push Mobile**.

Note :
Les utilisateurs bénéficiant d'un accès au Push Mobile doivent télécharger le client Push Mobile à partir du bureau virtuel ou du bureau virtuel mobile. Pour plus d'informations sur l'installation du client Push Mobile, reportez-vous au Guide Utilisateur correspondant.

11.2 Téléphonie SIP sur Internet

11.2.1 Introduction

Extended Communication Server vous offre un accès gratuit à la téléphonie sur le réseau Internet.

- Entre deux utilisateurs connectés au Bureau virtuel (à l'intérieur ou hors des locaux de la société). L'utilisateur connecté au Bureau virtuel fait appel à un softphone téléchargé et installé sur sa machine. Cette solution requiert Internet Explorer 6 (ou version ultérieure) ainsi que l'activation d'ActiveX.

  Pour mettre en œuvre cette solution, consultez la section § Configuration de base pour la téléphonie SIP sur Internet .

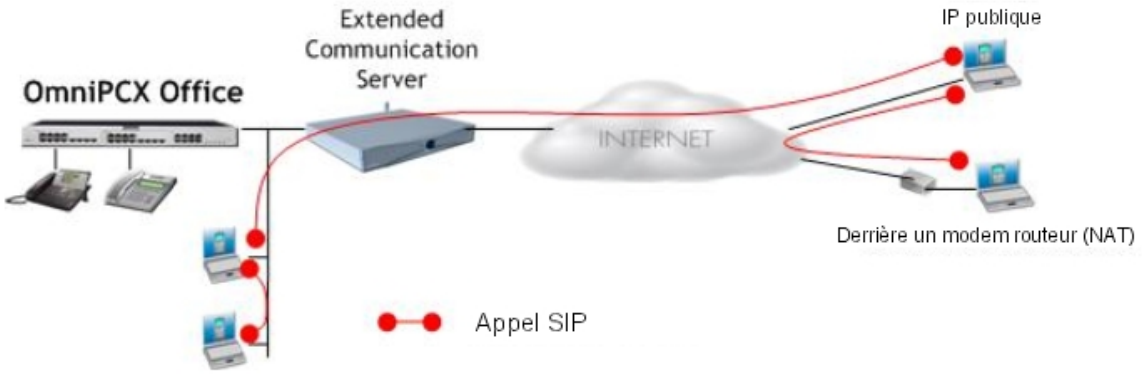


Figure 11.3 : Communications Peer to Peer (d'égal à égal)

- Entre un utilisateur connecté au Bureau virtuel et un utilisateur d'Alcatel-Lucent OmniPCX Office Communication Server. Cette solution requiert Internet Explorer 6 (ou version ultérieure) ainsi que l'activation d'ActiveX.

  Pour mettre en œuvre cette solution, consultez la section § Configuration d'interopérabilité avec OmniPCX Office .

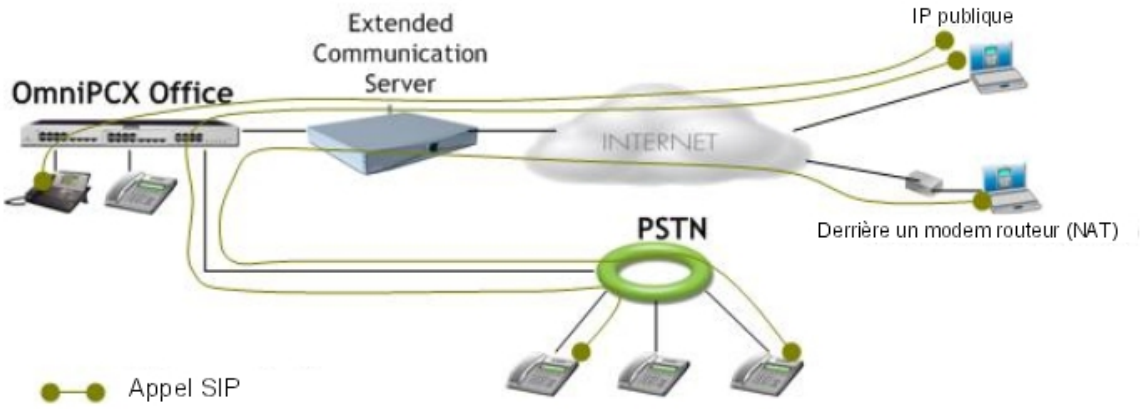


Figure 11.4 : Communications entre Bureau virtuel et OmniPCX Office

- Entre un internaute visitant le site Web de l'entreprise et un utilisateur d'Alcatel-Lucent OmniPCX Office Communication Server. L'internaute clique sur un bouton d'appel sur le site Web pour initier une communication. Lorsque l'internaute clique sur ce bouton pour la première fois, un plug-in est installé. Ce dernier requiert Internet Explorer 6 (ou version ultérieure) ainsi que l'activation d'ActiveX.

  Pour mettre en œuvre cette solution, consultez la section § Ajout d'un bouton Click to call sur le site Web .

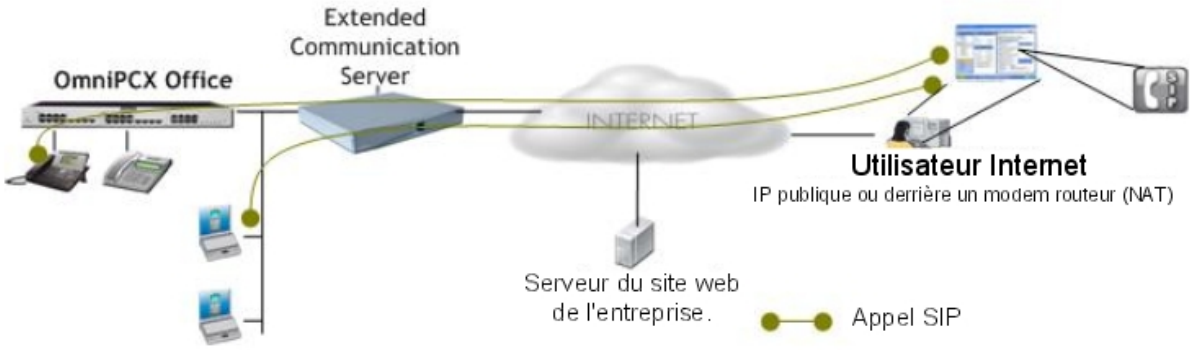


Figure 11.5 : Accessibilité Web

11.2.2 Configuration de base pour la téléphonie SIP sur Internet

À l'issue de cette section, vous saurez mettre en place la téléphonie SIP sur Internet entre deux utilisateurs connectés à leur Bureau virtuel.

Note :

Dans l'exemple ci-dessous, l'Extended Communication Server constitue le serveur DNS (Domain Name System) du nom de domaine utilisé dans le cadre de la téléphonie SIP sur Internet.

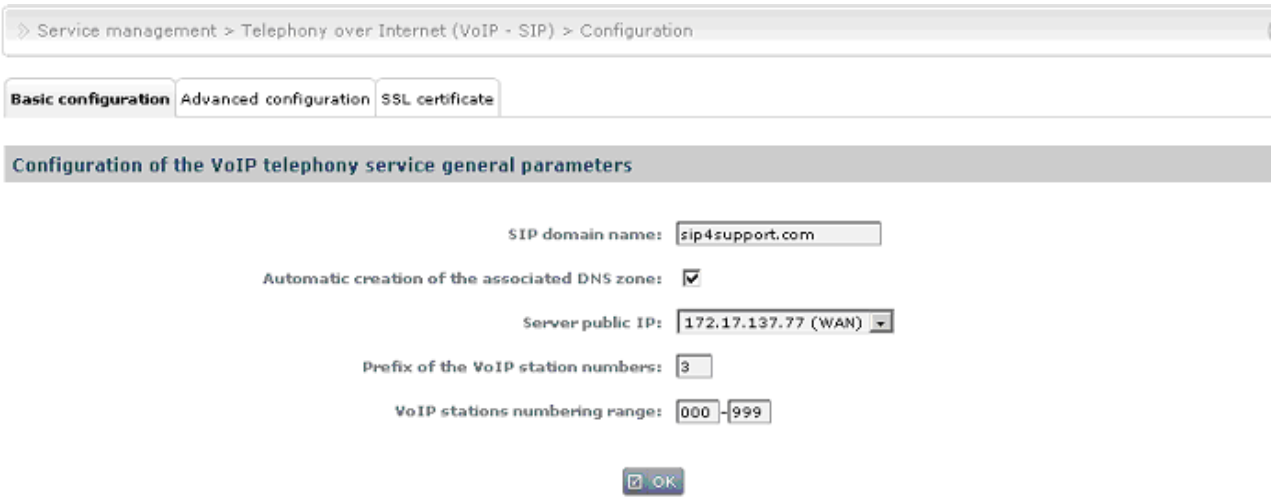
11.2.2.1 Pré-requis

- Le service DNS doit être activé sur l'Extended Communication Server.
- Vous devez créer un certificat associé au nom de domaine utilisé dans le cadre de la téléphonie SIP sur Internet. Pour plus de précisions sur la création de certificats, voir la section module Installation du système - Gestion de la sécurité § Création d'un certificat utilisateur .
- Vous devez autoriser l'accès des postes utilisateur situés derrière un firewall aux numéros de port suivants :
  - Port TCP 5061 de l'ordinateur à Internet
  - Plage TCP/UDP 8000:9000 de l'ordinateur à Internet

11.2.2.2 Activation de la téléphonie SIP sur Internet

Pour configurer et activer la téléphonie SIP sur Internet :

1. Sélectionnez le menu **Gestion des services** > **Téléphonie sur Internet (VoIP - SIP)** > **Configuration**.
2. Sélectionnez l'onglet **Configuration de base**.



3. Dans le champ **Nom du domaine SIP**, saisissez le nom du domaine à utiliser pour les adresses SIP. Ce domaine est géré par le serveur DNS de l'Extended Communication Server. Ce nom peut être identique au **Nom de domaine de l'Appliance**.
4. Activez la case à cocher **Création automatique de la zone DNS associée** afin que des champs spécifiques soient automatiquement ajoutés au DNS de l'Extended Communication Server.
5. Sélectionnez l'adresse **IP publique du serveur** dans la liste déroulante.
6. Dans le champ **Plage de numérotation des postes VoIP**, saisissez une plage comprenant au moins cent numéros.
7. Cliquez sur **OK**.
8. Sélectionnez l'onglet **Certificat SSL**.

9. Sélectionnez le certificat à utiliser pour le nom de domaine VoIP - SIP.
10. Activez le serveur de **téléphonie sur Internet**.

11.2.2.3 Configuration des droits d'accès utilisateur

Pour accorder ou refuser à un utilisateur le droit d'accéder à la téléphonie SIP sur Internet :

1. Sélectionnez le menu **Gestion des services** > **Téléphonie sur Internet (VoIP - SIP)** > **Configuration des postes VoIP**.
2. Pour chaque utilisateur, indiquez si vous souhaitez activer la téléphonie VoIP.

   Note :
   La téléphonie VoIP est activée par défaut pour tous les utilisateurs.
3. Cliquez sur **OK**.

11.2.3 Configuration d'interopérabilité avec OmniPCX Office

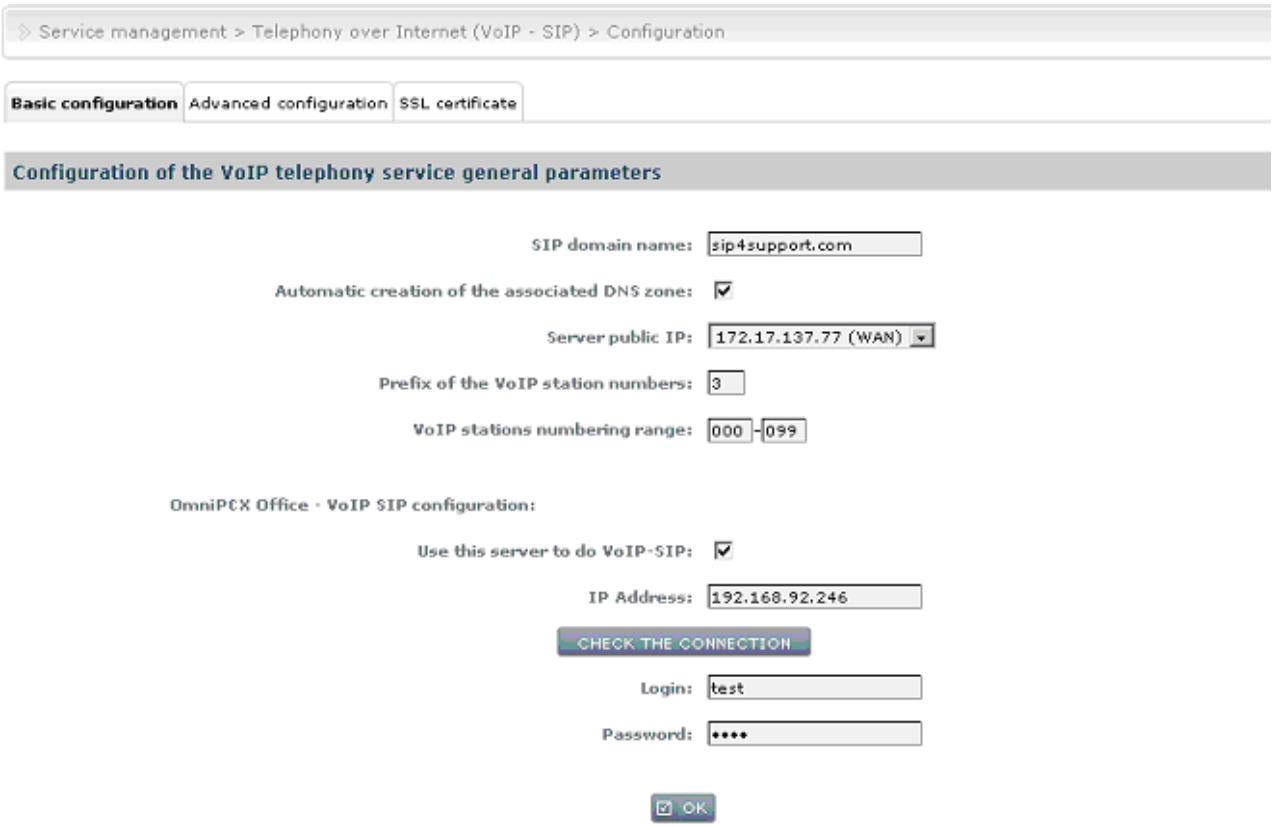
À l'issue de cette section, vous saurez mettre en place la téléphonie SIP sur Internet entre un utilisateur connecté à un Bureau virtuel et un utilisateur de l'OmniPCX Office.

11.2.3.1 Pré-requis

- Vous devez effectuer la configuration de base pour la téléphonie SIP sur Internet.
- Alcatel-Lucent OmniPCX Office Communication Server version 7.0 ou ultérieure est nécessaire et vous devez configurer la fonction de raccordement SIP.

11.2.3.2 Configuration de l'interopérabilité avec OmniPCX Office

1. Sélectionnez le menu **Gestion des services** > **OmniPCX Office** > **Détection et Configuration**.
2. Sélectionnez l'onglet **Détection IP**.
3. Cliquez sur le bouton **Détection de l'IP de l'OmniPCX Office**.
   Après quelques secondes, l'adresse IP de l'OmniPCX Office s'affiche à l'écran.
4. Cliquez sur **OK** et activez le service.
5. Sélectionnez le menu **Gestion des services** > **Téléphonie sur Internet (VoIP - SIP)** > **Configuration**.



6. Sous **OmniPCX Office - VoIP SIP configuration**, activez la case à cocher **Utiliser ce serveur pour faire de la VoIP-SIP**.
7. Dans le champ **Adresse IP**, saisissez l'adresse IP de la carte VoIP sur l'Alcatel-Lucent OmniPCX Office Communication Server.
8. Dans les champs **Login** et **Mot de passe**, saisissez le login et le mot de passe de la passerelle SIP sur l'Alcatel-Lucent OmniPCX Office Communication Server.
9. Cliquez sur **OK**.
10. Cliquez sur le bouton **Vérifier la connexion** afin de contrôler la configuration.

11.2.4 Ajout d'un bouton Click to call sur le site Web

À l'issue de cette section, vous serez en mesure d'ajouter un bouton Click to call afin que les visiteurs de votre site Web puissent appeler un utilisateur de l'OmniPCX Office.

11.2.4.1 Pré-requis

- Vous devez effectuer au préalable la configuration de base pour la téléphonie SIP sur Internet ainsi que la configuration d'interopérabilité avec l'OmniPCX Office.
- Vous devez avoir créé votre site Web à l'aide d'une version d'Extended Communication Server prenant en charge la téléphonie SIP sur Internet : voir la section module Installation

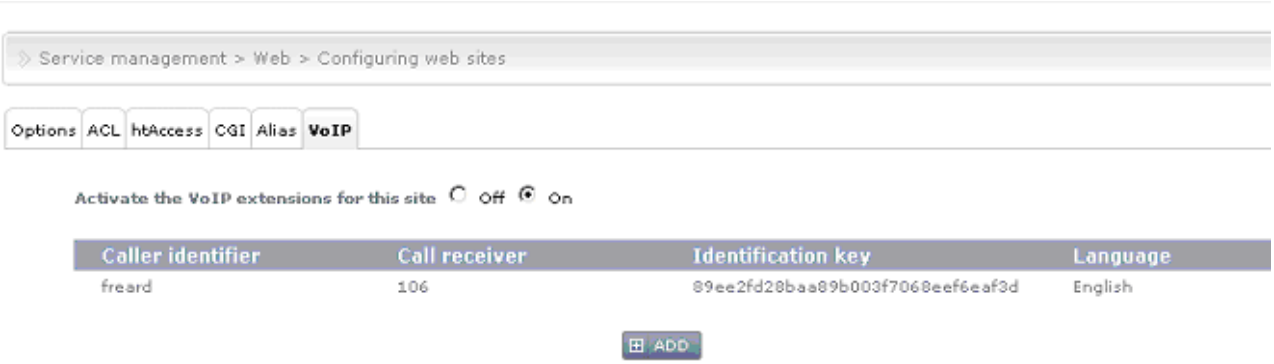
du système - Hébergement Web .

11.2.4.2 Obtention de la clé d'identification

Pour obtenir la clé d'identification associée à l'utilisateur qui reçoit les appels initiés à l'aide du bouton Click to call :

1. Sélectionnez le menu **Gestion des services** > **Web** > **Configuration des sites Web**.

2. Cliquez sur le bouton **Modifier** .
3. Sélectionnez l'onglet **VoIP**.



4. Sélectionnez **Activer les extensions VoIP pour ce site** en cliquant sur **On**.
5. Sélectionnez l'utilisateur qui doit recevoir les appels initiés à l'aide du bouton Click to call et cliquez sur **Ajouter**.
6. Copiez la **Clé d'identification** dans le Presse-papiers (ou dans un fichier texte). Cette clé permet de générer le code html du bouton Click to call.

11.2.4.3 Ajout du bouton Click to call sur le site Web

Pour ajouter un bouton Click to call sur le site Web :

1. Créez un fichier html comprenant le code suivant.

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8">
<title>Click to call</title>
<script language='javascript' src='/voip/softphone.js'></script>
</head>
<body>
<form>
<input type='button' value='Click to Call'
onClick='ctd("89ee2fd28baa89b003f7068eef6eaf3d")'>
```

Dans cet extrait, remplacez `Click to Call` par le texte qui doit apparaître dans le site Web sur le bouton Click to call et `89ee2fd28baa89b003f7068eef6eaf3d` par la **Clé d'identification** copiée lors de l'étape précédente à partir de l'interface d'administration.

```
</form>
</body>
</html>
```

2. Transférez le fichier html vers le serveur : voir la section module Installation du système - Hébergement Web § Chargement du site sur le serveur
3. Accédez au site Web et testez le bouton.

Chapitre

12

Sauvegarde et restauration

À l'issue de ce chapitre, vous saurez comment sauvegarder la configuration et les données de l'Extended Communication Server, pour ensuite restaurer tout ou partie de celles-ci si nécessaire.

12.1 Généralités

La fonction de sauvegarde de l'Extended Communication Server vous permet d'enregistrer à la fois la configuration et les données du serveur, y compris les paramètres et données associés à chaque compte utilisateur.

Nous vous recommandons d'effectuer une sauvegarde manuelle après la première installation et après chaque modification majeure de la configuration. Par ailleurs, vous pouvez programmer des sauvegardes automatiques afin d'enregistrer régulièrement les données les plus récentes, notamment les paramètres et les données associés aux comptes utilisateurs.

La fonction de sauvegarde fournit plusieurs options, parmi lesquelles :

- des profils de sauvegarde personnalisés,
- la détection automatique des périphériques de stockage,
- la sélection des périphériques de stockage (stockage sur plusieurs périphériques et sur machine distante),
- des sauvegardes totales ou différentielles,
- le cryptage des archives,
- la compression des archives,
- la rotation des archives,
- la planification des sauvegardes.

La fonction de restauration vous permet de restaurer l'ensemble des paramètres et données de configuration, ainsi que de naviguer dans une archive afin de sélectionner précisément les éléments à restaurer.

12.2 Procédure de sauvegarde

La procédure de sauvegarde s'articule autour de deux étapes :

1. Définition d'un profil de sauvegarde
2. Exécution d'une sauvegarde préalablement définie

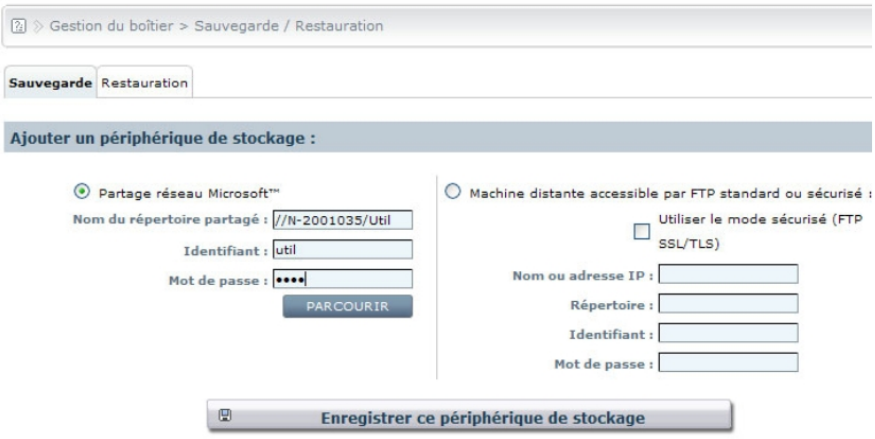
12.2.1 Définition d'un profil de sauvegarde

Pour définir un profil de sauvegarde :

1. Sélectionnez le menu **Gestion du boîtier > Sauvegarde / Restauration**.
2. Sélectionnez l'onglet **Sauvegarde**.

Gestion du boîtier > Sauvegarde / Restauration
Sauvegarde
Restauration
Liste des profils de sauvegarde :
Ajouter un profil de sauvegarde

3. Cliquez sur **Ajouter un profil de sauvegarde**.
   Un profil de sauvegarde définit un ou plusieurs périphériques de stockage, ainsi que les caractéristiques de l'opération de sauvegarde.
4. Cliquez sur **Ajouter un périphérique de stockage**.
   Les périphériques disponibles sont automatiquement détectés. Par défaut, le formulaire propose les options de partage du réseau et d'accès distant. Lorsque d'autres périphériques (USB, par exemple) sont détectés, ils apparaissent également dans le formulaire de sélection.
5. Sélectionnez le périphérique de stockage.
6. Cliquez sur **Enregistrer ce périphérique de stockage**.
   Avant que ce périphérique ne soit accepté, le système vérifie si les données peuvent être stockées. Dans la négative, modifiez les paramètres et réessayez.


Gestion du boîtier > Sauvegarde / Restauration
Sauvegarde
Restauration
Ajouter un périphérique de stockage :
Partage réseau Microsoft™
Nom du répertoire partagé : //N-2001035/Util
Identifiant : util
Mot de passe :
PARCOURIR
Machine distante accessible par FTP standard ou sécurisé :
Utiliser le mode sécurisé (FTP SSL/TLS)
Nom ou adresse IP :
Répertoire :
Identifiant :
Mot de passe :
Enregistrer ce périphérique de stockage

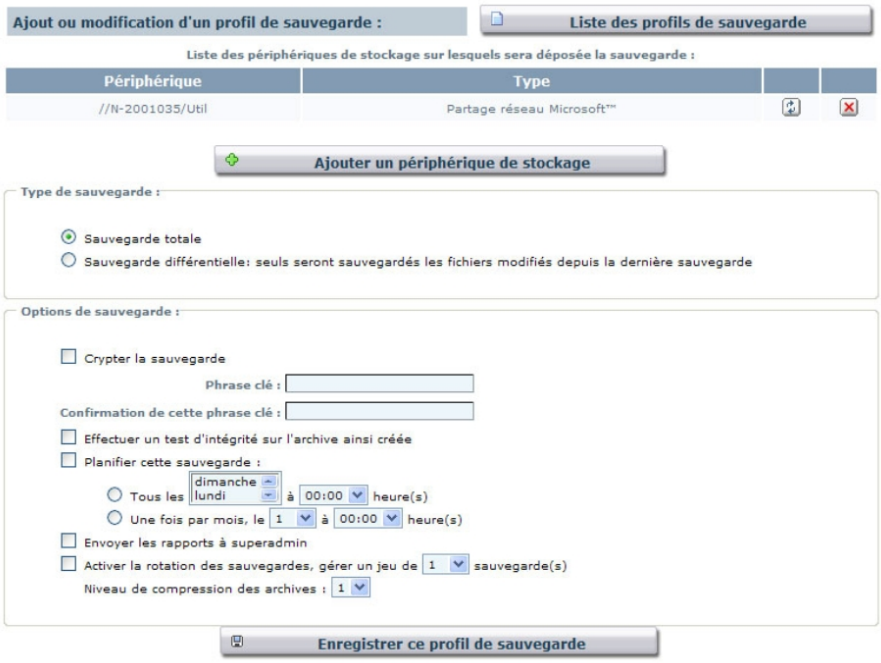
Notes :
Les noms de répertoire doivent respecter la casse.

Utilisez le caractère « / » comme séparateur dans le chemin d'accès.

Assurez-vous que le périphérique de stockage cible est accessible en lecture/écriture et qu'il dispose d'un espace libre suffisant.

Assurez-vous également que les paramètres de sécurité autorisent l'accès au périphérique souhaité.

7. Définissez le type de sauvegarde :
   - Une sauvegarde totale stocke tous les fichiers, à l'exception des logs.
   - Une sauvegarde différentielle stocke seulement les fichiers ayant été modifiés depuis la dernière sauvegarde.
8. Définissez les options de sauvegarde (cryptage, planification, compression, etc.). Reportez-vous à l'aide en ligne pour plus de détails.


Ajout ou modification d'un profil de sauvegarde :
Liste des profils de sauvegarde
Liste des périphériques de stockage sur lesquels sera déposée la sauvegarde :
Périphérique
Type
//N-2001035/Util
Partage réseau Microsoft™
Ajouter un périphérique de stockage
Type de sauvegarde :
Sauvegarde totale
Sauvegarde différentielle: seuls seront sauvegardés les fichiers modifiés depuis la dernière sauvegarde
Options de sauvegarde :
Crypter la sauvegarde
Phrase clé :
Confirmation de cette phrase clé :
Effectuer un test d'intégrité sur l'archive ainsi créée
Planifier cette sauvegarde :
Tous les dimanche lundi à 00:00 heure(s)
Une fois par mois, le 1 à 00:00 heure(s)
Envoyer les rapports à superadmin
Activer la rotation des sauvegardes, gérer un jeu de 1 sauvegarde(s)
Niveau de compression des archives : 1
Enregistrer ce profil de sauvegarde

9. Cliquez sur **Enregistrer ce profil de sauvegarde**.

12.2.2 Exécution d'une sauvegarde

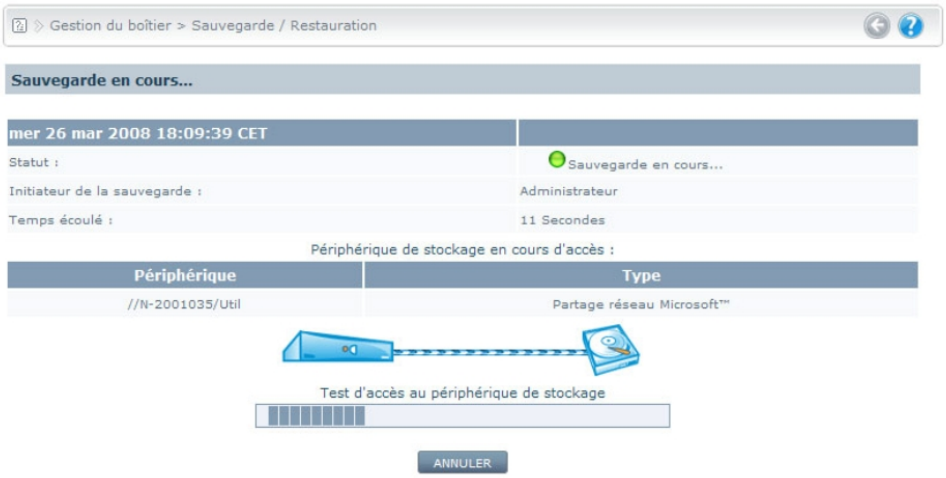
Dès l'instant où un profil de sauvegarde au moins est défini, vous pouvez exécuter une sauvegarde.

Pour exécuter une sauvegarde :

1. Sélectionnez le menu **Gestion du boîtier > Sauvegarde / Restauration**.
2. Sélectionnez l'onglet **Sauvegarde**.
   Les profils de sauvegarde existants apparaissent dans la liste.

3. Cliquez sur le bouton **Lancer la sauvegarde** associé au profil souhaité.
   Le système s'assure tout d'abord qu'il peut accéder au périphérique de stockage, puis exécute la sauvegarde.

Un panneau vous tient informé de l'avancement de la sauvegarde.



4. Patientez jusqu'à la fin de la procédure de sauvegarde.
   Une fois la sauvegarde terminée, le champ **Statut** vous indique que la sauvegarde a réussi.
5. Cliquez sur **VALIDER**.

12.3 Procédure de restauration

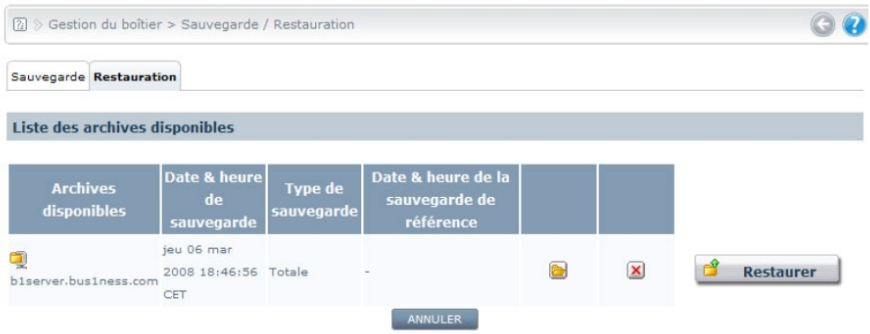
La procédure de restauration standard est facile à exécuter ; vous avez uniquement à désigner l'archive et à lancer la restauration.

L'exemple ci-dessous vous explique comment utiliser une fonction avancée du programme de restauration. Le but de cette procédure est de restaurer les e-mails d'un seul utilisateur, dont l'identifiant est *sbogdani*.

Pour restaurer les e-mails d'un utilisateur :

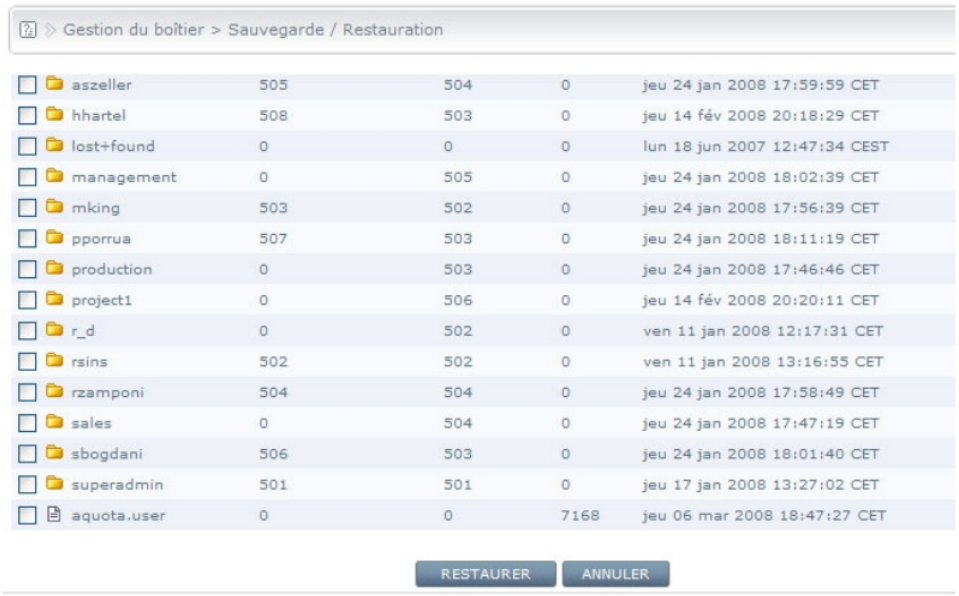
1. Sélectionnez le menu **Gestion du boîtier > Sauvegarde / Restauration**.
2. Sélectionnez l'onglet **Restauration**.
   La liste des périphériques de stockage s'affiche.

3. Cliquez sur le périphérique de stockage souhaité.
   La liste des archives disponibles s'affiche.



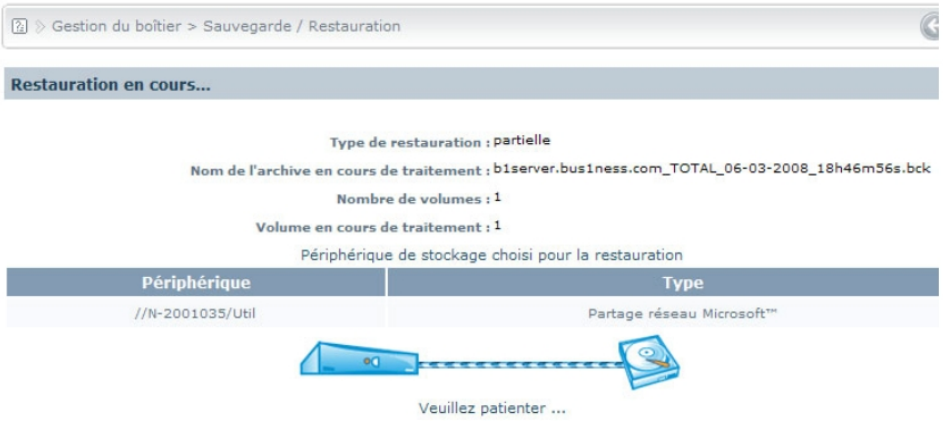
Note :
*Si vous cliquez sur le bouton **Restaurer** à ce stade, l'intégralité de l'archive est restaurée.*

4. Cliquez sur le bouton pour accéder aux répertoires et aux fichiers d'archivage.


Gestion du boîtier > Sauvegarde / Restauration
aszeller 505 504 0 jeu 24 jan 2008 17:59:59 CET
hhartel 508 503 0 jeu 14 fév 2008 20:18:29 CET
lost+found 0 0 0 lun 18 jun 2007 12:47:34 CEST
management 0 505 0 jeu 24 jan 2008 18:02:39 CET
mking 503 502 0 jeu 24 jan 2008 17:56:39 CET
pporrua 507 503 0 jeu 24 jan 2008 18:11:19 CET
production 0 503 0 jeu 24 jan 2008 17:46:46 CET
project1 0 506 0 jeu 14 fév 2008 20:20:11 CET
r_d 0 502 0 ven 11 jan 2008 12:17:31 CET
rsins 502 502 0 ven 11 jan 2008 13:16:55 CET
rzamponi 504 504 0 jeu 24 jan 2008 17:58:49 CET
sales 0 504 0 jeu 24 jan 2008 17:47:19 CET
sbogdani 506 503 0 jeu 24 jan 2008 18:01:40 CET
superadmin 501 501 0 jeu 17 jan 2008 13:27:02 CET
aquota.user 0 0 7168 jeu 06 mar 2008 18:47:27 CET
RESTAURER
ANNULER

5. Ouvrez le répertoire de messagerie (*_services_/cyrus/spool/mail*).
6. Comme *sbogdani* commence par un s, sélectionnez le répertoire **s**.
7. Sélectionnez le répertoire **user**.
   Tous les e-mails de l'utilisateur sont stockés dans ce répertoire.

8. Cochez la case correspondant à l'utilisateur.
9. Cliquez sur **Restaurer**.
   Une confirmation est demandée.
10. Cliquez sur **Restaurer**.
    La procédure de restauration est lancée.


Gestion du boîtier > Sauvegarde / Restauration
Restauration en cours...
Type de restauration : partielle
Nom de l'archive en cours de traitement : b1server.bus1ness.com_TOTAL_06-03-2008_18h46m56s.bck
Nombre de volumes : 1
Volume en cours de traitement : 1
Périphérique de stockage choisi pour la restauration
Périphérique
Type
//N-2001035/Util
Partage réseau Microsoft™
Veuillez patienter ...

11. Patientez jusqu'à la fin de la procédure de restauration.
12. Une fois la restauration terminée, cliquez sur **Valider**.

Chapitre

13

Annexes

13.1 Comment établir un devis

Utilisez l'outil Actis pour établir le devis d'une solution incluant l'Extended Communication Server. Aucune option spécifique n'est requise. Il vous suffit d'établir le devis d'une solution Extended Communication Server standard, en indiquant le nombre d'utilisateurs finaux qui utiliseront les services de l'Extended Communication Server, tel qu'illustré ci-dessous.

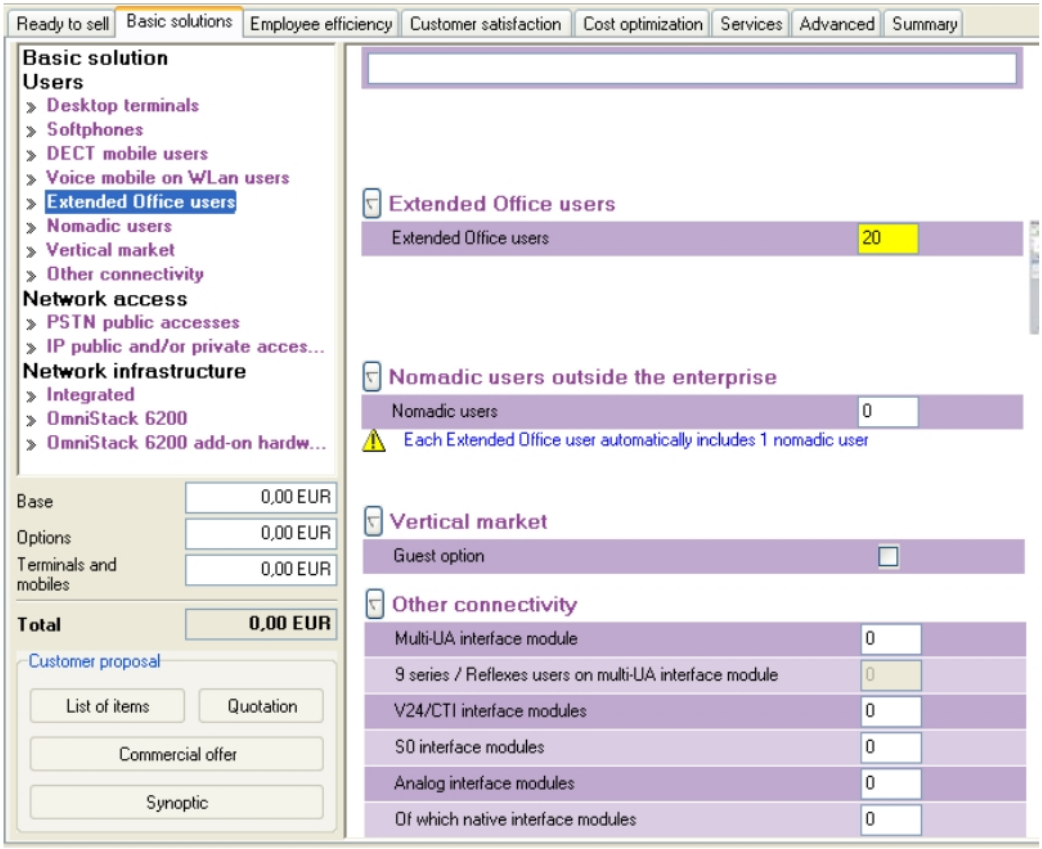


Figure 13.1 : Comment établir un devis à l'aide d'Actis

13.2 Comment commander

Pour commander un Extended Communication Server, accédez au site Web Alcatel-Lucent Business Partner à l'adresse suivante : http://www.businesspartner.alcatel-lucent.com/. Sélectionnez le menu **ONLINE SERVICES > eBuy > Ordering rules > Alcatel Eye-box**. Reportez-vous ensuite au guide de saisie de commande de l'Extended Communication Server.

Chapitre 13 *Annexes*